A CRITICAL REVIEW OF THE IMPLEMENTATION OF THE SECURITY THREAT ASSESSMENT BY A SELECTION OF GOVERNMENT DEPARTMENT IN GAUTENG

by

LEHLOHONOLO WONDERBOY MAHLATSI

submitted in accordance with the requirements for the degree of

DOCTOR OF LITERATURE AND PHILOSOPHY

in the subject

CRIMINAL JUSTICE

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: DR B.K. LEKUBU

November 2022

DECLARATION

Name: Lehlohonolo Wonderboy Mahlatsi

Student Number: **43312829**

Degree: **Doctor of Literature and Philosophy in Criminal Justice**

A Critical Review of the Implementation of the Security Threat Assessment by a Selection of Government Departments in Gauteng.

I declare that the above thesis is my own work, and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I submitted the thesis to originality checking software and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

16/09/2022

SIGNATURE DATE

DEDICATION

I dedicated my previous postgraduate research posthumously in memory of my late sister, Puleng Cynthia Mahlatsi, whom I adored profusely. Her death in 2016 left my mother with irreparable physical, emotional, and psychological scars. The current research study is then dedicated to my mother, Susan Pinky Mahlatsi, whose immeasurable sacrifices are visible in my children's eyes. My life and academic goals are poignantly focused on my completion of my doctoral studies for her to see me wearing the red academic gown as a reward for her endless sacrifice.

NDIYABULELA MAMA!!!

ACKNOWLEDGEMENTS

Hake qale ka bohlale bo boholo, ke lebohe bophelo. Ke lebohe Modimo Ntate, Modimo Mora, le moya o halalelang. I thank God in the name of Jesus Christ, my Comforter, the Lion King of Juda; God Messiah to our parents, God Messiah to us, God Messiah to our children and their children in the future.

Secondly, I would like to take this opportunity to express my heartfelt and profound gratitude to the following people:

1. My father, Priest Mokete Joseph Mahlatsi. He was right that a man must establish his position in the house, church, community, work, and in the academic sphere. **Vitória é certa** (Victory is certain).
2. To my brothers, Lebo and Sabata Mahlatsi, my sister 'Mazzet', my cousins, nephews, and nieces, for your infinite love and continuous encouragement. **Aluta continua.**
3. My in-laws, Mr and Mrs Mokheseng, for remembering me in their prayers, and for their loyal support. **Kea leboha**.
4. My supervisor, coach, and mentor, Dr Benni Khotso Lekubu for his commitment and excellent mentorship. He has selflessly inspired and empowered me, the son of a domestic worker and a taxi driver. Thank you, Sir, for your continuous guidance and support throughout my studies. **#Blackexcellence**.
5. The editor, Dr Themba J. Mkhonto. I wish to express my sincere appreciation of his dedication and efforts. **"A man who wants to lead the orchestra, must turn his back on the crowd" (Max Lucado).**
6. To all my research participants, I want to thank you with all my heart**. I am because you are.**
7. To Ms Diana Rakoma, my friend and colleague for always being available to assist **Ndo livhuwa Khaladzi.**
8. I was born and raised in love, and understand what it means to be loved and embraced by my parents and siblings. I never imagined that anyone else would love me as much as they did. Accordingly, I thank my wife and friend, Mrs. Maki Jerminah Mahlatsi, 'naledi ya Tau', for blessing me with two lovely daughters, Lerato and Leano Mahlatsi. Thank you for your patience and understanding during the most trying moments of my studies. May God remember you like Noah, protect you like David, resurrect you like Jesus, and let his will be your wheel always. **Kea leboha Mabanyana.**
9. To my beautiful girls, Lerato and Leano, let the people see my work through you. Tau e fihlile.

ABSTRACT

The imperative for protecting critical national infrastructure has engendered development of the Security Threat Assessment Framework that is implemented by the South African government under the guidance of the State Security Agency (SSA). The objective of the STRA Security Threat Assessment Framework is to detect any weaknesses in existing security measures, and to recommend strategies to evaluate ameliorative improvements in those identified weaknesses. The aim of the study is to critically review the implementation of the security threat assessment by a selection of government Department in Gauteng.

The study has adopted a qualitative research design approach due to its constructivist-interpretivist inspiration and reliance on participant-centred mode of acquiring the study's pertinent primary data through document analysis, semi-structured in-depth interviews with the primary participants, and observations with secondary participants. The study population comprised of security managers, vetting managers, cybercrime managers, information security managers, physical security managers, and professionals in the security environment. Additionally, the target population and sample size consisted of 47 participants from various spheres of the security sector locally. These participants were selected through the purposive and simple random sampling strategies respectively.

Some of the study's critical findings show that there was general awareness and knowledgeability concerning the appointment processes and roles of security managers and security committees. The role of technology was viewed as beneficial. As such, the security of sensitive information necessitated that personnel working in high-risk environments as well as personnel in charge of information technology systems should be subjected to security procedures. These procedures include declaration of secrecy, security profile checks of each user, limiting access to top secret to individuals nearing retirement or exiting the system; as well as backup of the sensitive information in case it may be tampered with.

Key words: threat, risk, vulnerability, legal mandate, exploit, impact, information security, South African Government Departments, cybersecurity, counter-intelligence, classified information

ABBREVIATIONS

AFATAP	African Association of Threat Assessment Professionals
AGSA	Auditor-General of South Africa
APIs	Application Programming Interfaces
BRICS	Brazil, Russia, India, China, and South Africa
CAPPVA	The Control of Access to Public Premises and Vehicles Act 53 of 1985
CCCS	Canadian Centre for Cyber Security
CCMA	Commission for Conciliation, Mediation, and Arbitration
CCTV	Closed-circuit Television
CERT	Community Emergency Response Team
CIAC	Crime Information Analysis Centre
CCF	Crime Combating Forum
CNS&AP	Canadian National Strategy and Action Plan for Critical Infrastructure
CPS	Cash Paymaster Services
CSIRC	Canadian Security Intelligence Review Committee
CTA	Crime Threat Assessment
DAST	Dynamic Application Security Testing
DIRCO	Department of International Relations and Cooperation
DOJ & CD	Department of Justice and Constitutional Development
DPSA	Department of Public Service and Administration
DTI	Department of Trade & Industry
DWAF	Department of Water Affairs and Forestry
ETDP	Education Training Development Practitioner
ERM	Enterprise Risk Management
EU	European Union
FCA	Firearms Control Act
GSR	Government Security Regulator
IBM	International Business Machines
ICT	Information Communication Technology
ISO	International Organization for Standardization
ISS	Islamic State
MISS	Minimum Information Security Standards
MPSS	Minimum Physical Security Standards
NIA	National Intelligence Agency
NCTA	National Cyber Danger Assessment
NTAC	National Threat Assessment Centre
OECD	Organisation for Economic Cooperation and Development

PAD	Protected Disclosures Act
PSIRA	Private Security Industry Regulatory Act
PSSD	Protection and Security Services Division
RSA	Republic of South Africa
SA	South Africa
SALRC	South African Law Reform Commission
SANDF	South African National Defence Force
SAPS	South African Police Service
SARB	South African Reserve Bank
SASSETA	Safety and Security, Sector Education & Training Authority
SITA	State Information Technology Agency
SAST	Static Application Security Testing
SOPs	Standard Operating Procedures
SSA	State Security Agency
STAF	Security Threat Assessment Framework
STRA	Security Threat Risk Assessment
STRAF	Security Threat Risk Assessment Framework
SSR	Security Sector Reform
STA	Security Threat Assessment
TSC	Top Security Clearance
TSCM	Technical Surveillance Counter Measure
TUT	Tshwane University of Technology
UK	United Kingdom
UNISA	University of South Africa
VBS	Venda Building Society

Table of Contents

List of Tables

List of Figures

CHAPTER 1
GENERAL ORIENTATION

1.1 INTRODUCTION

The national priorities and interests of South Africa (SA) are within the custodial responsibility of national, provincial, and local government departments (Department of Public Service and Administration, 2016: 7). South Africa is an emerging democratic country working closer with countries that aspire to assume competitive economic and political status against other established economies globally. South Africa's membership in the Brazil, Russia, India, China, and South Africa (BRICS) organisation signifies an orientation towards political autonomy and economic competitiveness (Department of International Relations and Cooperation (DIRCO) (South Africa, 2021: 1). In addition to economic advantage, SA also acknowledges the strategic viability of such partnerships, despite the disparate national agendas or priorities among the BRICS Member States. In that regard, the DIRCO fulfils a leading role on behalf of the SA government and has the custodial care of responsibilities and all other relevant information pertaining to all facets of the country's involvement in the BRICS multilateral structure (South Africa, 2021: 1).

The Minimum Information Security Standard (MISS) emphasises the need for stringent security controls to protect the highly sensitive information that is vested in the custody of all government departments (SA, 1998: 1). Competing international developments necessitate that government departments should fulfil their respective mandates in order to mediate the plethora of local and international security threats (Ameer-Mia & Shacksnovis, 2019: 137). Moreover, the perpetual quest for global competitive advantage has heightened the need for countries to engage in complex cyber security arrangements for protecting their own territorial integrity and sovereignty (Broder & Tucker, 2012: 13).

It is in this context that the government departments should necessarily maintain open global internet systems and programmes with sufficient capability to detect and deter cyber-attacks and related threats from other countries (Antinyan, Staron, Sandberg & Hansson, 2016: 1). Such systems and programmes are advantageous insofar as they provide government departments with the requisite response frameworks to prioritise and counter specific threats, as well as proactively determining the exposure levels of assets of the State (Sutherland, 2017: 20).

The imperative for protecting critical national infrastructure has engendered development of the Security Threat Assessment Framework (STAF) which the South African Government can use under the guidance of the State Security Agency (SSA) (South Africa, 1994: 1). The STA's objective is to detect any weaknesses in existing security measures, and to recommend strategies to evaluate ameliorative improvements in those identified weaknesses (Allen, 2016: 4). However, the high number of internal and external security breaches in South Africa is ample demonstration that the government departments are confronted with the mountainous challenge of dealing with threats and attacks that are rapidly becoming more sophisticated and have taken a major shift in digital infrastructure requirements (Ameer-Mia & Shacksnovis, 2019: 137). These ominous threats are organised from inside and outside the country, and they pose a danger to assets of the State and national security, the people and critical infrastructure; as well as essential information held by government departments (South Africa, 2001: 1; Sutherland, 2017: 20)

Inadequacy of proper security structures and programmes is not uniquely South African, but common even among well-developed national economies across the globe (Council of Europe, 2001: 1). For example, in the United Kingdom (UK) alone, about 8,995 security breaches occurred in 17 of the largest government departments, yet they do not have standard operation procedures and frameworks component and methodology to report them (Palmer, 2016: 12). Maintaining a correct level of protecting critical national assets and infrastructure and deterrence against foreign and domestic threats requires commitment from each department, against whose objectives the risks are identified and measured (Allen, 2016: 58). Risk assessment should be incorporated as a major aspect of the STA report, particularly at those facilities where the likelihood of threat has not been identified already. This will have enormous financial implications to the department, as a result of which it is important to comprehend such implications before concluding the risk or threat assessment details in the security plan (Garcia, 2006: 12; Pinnock, 2020: 1).

The above-cited passages in this introductory section have actually presaged and highlighted the study's aim or purpose, which is: to critically review the implementation of the security threat assessment by a selection of government Department in Gauteng. Such investigation (exploration, description and analysis) will provide insight on the extent of these departments' prioritisation of the counter-intelligence strategies and implementation of the STA. Such research-based investigation will further provide some degree of definitive conceptualisation of critical aspects, such as: personnel security, valued assets, and crucial information of the State; as well as the requisite balance between the value of the assets and the amount of money that needs to be spent on the layers of security measures (Patrick, van Niekerk & Fields, 2016: 68). Most importantly, this proposed study also seeks to determine the extent of clarity between categories of information regarded as crucial, and those (information categories) that are deemed to fulfil the requirements of classification (Adetiba, 2017: 220).

1.2 BACKGROUND OF THE STUDY

Security and management of risk comprises of two elements (Rishi, 2019: 1; Sutton, 2015: 14). Firstly, that there is a likelihood of a loss to assets or harm occurring. Secondly, that the asset value itself ought to be safeguarded. Therefore, South African government departments ought to effectively implement the STA counter-intelligence tool to assist them in defining the nature of the threat being encountered, establishing the type of compromise involved, and the probability of each compromise (South Africa, 2017: 1). In this regard, the STA serves the fundamental purpose of determining adequacy of security measures from the perspective of requirements, efficiency, and cost (Maillart, 2014: 7). In the case of South Africa, there is generally ineffective implementation of the STA and correct application of its recommendations (South Africa, 2016: 1).

Saleh, Refai and Mashhour (2011: 87) argue that there are many benefits and shortcomings that are associated with assessment of threats and risks. In that regard, the STA should be of assistance in changing and improving the existing security controls, while also providing a comprehensive view and assessment of current security risks. According to Philpott (2013: 231), a threat assessment is a security appraisal of actions that can be harmful and negatively impact the core organisational business. Meanwhile, Black (2010: 471) alludes that a threat assessment is a framework-based mechanism mostly utilised by the government and commercial sectors, as well as most security industry experts, and operates according to the prescripts of the law. Threat assessment procedures could be in the form of definite and thoroughly composed records, or essentially, consciousness of the potential dangers from different circumstances. Security officers use the information from their records to ascertain the authenticity, correctness, and possible consequences of the risk or threat (African Union Convention, 2014: 1; Ramluckan, 2019: 348).

Philpott (2013: 231) further identifies the main reasons that necessitate threat assessment as attributable to factors such as the historic information of departments, including activities that are criminally motivated and have a link to terrorists. The researcher agrees with Philpott (2013: 231), that the institutional memory of departments is a very important source for assessment of threat and management of risk. The Minimum Physical Security Standards (MPSS) provides guidelines on the physical security requirements and other methods of installations (South Africa, 2009). The MPSS shows further that the minimum standards are necessary, despite problems concerning their legal enforceability, and constitute a point of departure towards binding regulations (South Africa, 2009).

The requirements and concomitant standards for threat and risk assessment basically seek to foster government departments' understanding of *what* needs to be protected, nature and level of the threats and vulnerabilities in *what* is to be protected, any harmful implications, and what could be done to reduce or eliminate exposure to the loss or damages (Bayne, 2020: 9). According to Watts (2017: 19), a threat or risk portends loss, harm, or damage when a weakness or vulnerability is exploited. The potential for risk can be reduced by creating and implementing a threat and risk assessment as a risk management plan or strategy. The researcher agrees with Watts (2017: 19), that South African Government departments inevitably suffer financial loss and damage because of business disruption, reputational damage, loss of privacy; as well as legal implications due to loss of life when threats and risks are unknown.

The risk or threat monitoring procedure depends on the consequences of the developed risk assessment models, in terms of which reports are delivered to show all cautions regarding every conceivable danger (Rishi, 2019: 1). Furthermore, the monitoring is persistently rehashed to safeguard the advancement of a viable security framework, and a suitable move is made to address the risks related to those threats, which should necessarily improve the security framework (Amundrud, Aven & Flage-First, 2017: 7). Likewise, the risk assessment standards ought to be founded on the basis of the process of reporting (Saleh, 2011: 84). Ultimately, security managers will utilise a summarised report on the status and execution of the security in the department, after which the executives will review the security framework and strategies to reduce potential security vulnerabilities, and in this manner, improve the security framework (Saleh, 2011: 85).

In 2003, the South African Cabinet approved the mandated functions and broad structure of the new Protection and Security Services Division (PSSD) of the South African Police Service (SAPS) (South Africa, 2017: 1). These functions have led to establishment of the Component: South African Government Security Regulator (GSR) within the State's organisational architecture. Among some of its functions, the GSR is responsible for regulating the services of all existents and newly identified strategic installations and the administration of the National Key Points Act (No 102 of 1980) (South Africa, 1980: 1). The GSR is also responsible for all government entities, excluding the National Intelligence Agency (NIA), the South African Defence Force (SANDF) and the SAPS. The mandate of the GSR is to develop and implement the MPSS as an official document and to ensure that all government departments and institutions use it to comply and maintain their physical infrastructure. At the point when a threat assessment is concluded, such assessment may be imparted to the SAPS or the State Security Agency, depending on the nature and level of the threat (South Africa, 1980: 1).

While the SAPS oversees services rendered to government departments to ensure implementation of effective physical security measures and screening adherence thereto, the SSA is similarly capable of rendering information security and counter-intelligence services (South Africa, 1980: 2). According to the MISS (1998), the NIA cannot 'outsource' its own information and physical infrastructure security, and provides advisory, auditing, exercising and co-ordination of information security in the public, private, and parastatal South African sectors, not including the SAPS and the SANDF.

On the other hand, the private sector security is mandated by the Private Security Industry Regulatory Act (PSIRA) (No. 56 of 2001), which was established in terms of Section 2 of the Act (South Africa, 2001). The objectives of the PSIRA include regulation of the private security sector and provision of effective control measures in their private and public sector practices. The PSIRA is considered relevant to this study insofar as it relates to its (PSIRA's) role in providing security-related services to South African government departments, as well as the national interest (loyalties) of the private security industries in South Africa (South Africa, 2001: 1).

The National Key Points Act 102 of 1980 was enacted for the protection of all national strategic areas of importance from being sabotaged (South Africa, 1980: 1). Moreover, a problem arose in South Africa in 2015 when some National Key Point breaches were undeclared until the Right2Know Campaign won its case at the Johannesburg High

Court (Right2know, 2015: np). The SAPS was subsequently ordered by the court to disclose the list of protected areas within 30 days of its ruling. In this court case, the major issues were the validity or otherwise of the National Key Points Act 102 of 1980 (SA, 1980) and its connection to the apartheid government (Thoka, 2021: 3).

1.3 PROBLEM STATEMENT

The previous section introduced the overall parameters of the research topic and culminated in an indication of the overall intention of this study. In the current section (Section 1.3), two critical research variables are entailed, namely: the rationale of the research study, and the problem that the researcher has identified as justification for the proposed research to be conducted. The rationale and research problem are then viewed as foundational to locating the research setting at which the exploration will occur, as well as the pre-exploration (pre-investigation) situational analysis to adequately comprehend the ontological state of the problem and its effects, consequences, and implications if left unresolved (Denscombe, 2014: 51- 52; Thanh & Thanh, 2015: 25).

The problem statement refers specifically to the articulation of the problem, or a description of a particular problematic situation or phenomenon (. Therefore, the problem with which the study is concerned is situated in the inadequate implementation of security threat or risk assessment framework measures by government departments. This problem is manifold and manifests itself in the weakening or already weakened capacity of government departments; information and communication technology (ICT) non-compliance and severity of security breaches; as well as poor monitoring and assessment of applicable policy frameworks (South Africa, 2017: 1). It is the inherent responsibility of government departments to develop implementable security threat programmes and policies to detect and avert all incidences linked to criminal and security breaches (Sutton, 2015: 11).

All government departments have their respective visions, missions, strategic objectives and mandates, which collectively characterises the form and extent of vulnerability of their physical and non-physical assets (Odendal, 2021: 14; Surju, 2018: 46). These objectives incorporate definition of the threat, identifying the target, and facility classification. However, the researcher has observed that the application of the STA and standard of the departmental reports are inimical to the objectives of the protection system. Additionally, the South African State Capture Commission has exposed the glaring weaknesses that are apparent in virtually all government departments and organs of State (Cawthra, 2019: 224).

Some of the machinations of hollowing-out and weakening the capacity of the affected departments included: extensive corruption at the Executive level throughout all organs of the State; factional politicisation of the intelligence, policing, and prosecution system/ apparatus; and vulnerability in governance due to re-purposing of departmental mandates (Cawthra, 2019: 225). Such a situation was fundamentally inimical to Security Sector Reform (SSR) and the State's service delivery mandate to citizens (South Africa, 1994: 1). Also, such service delivery shortfalls rendered the State vulnerable to both internal and external security threats and attacks. External threats include organised crime syndicates, activists, and foreign intelligence agencies. Internal threats could originate from disgruntled employees, unintended disclosures, sabotage, and acts of espionage. These criminal incidences and threats are induced mostly by asset vulnerabilities and security weaknesses (Sharma, 2020: 1).

Furthermore, some of these departments lack the strategies to protect the valued information and assets of government before they are rendered vulnerable and consequently compromise the preservation of integrity, availability, and confidentiality of information (Right2know, 2017: 1). Such departmental inefficiencies demonstrate a lack of institutional security policies, frameworks, standard operational procedures and different strategies and systems to secure their information. The 2013/2014 report of the Auditor General of South Africa (AGSA) made repetitive findings concerning ICT deficiencies within government departments (Nkwana & Govender, 2017: 18).

In this regard, the report cited shortfalls and deficiencies such as: internal ICT policy non-compliance or poor implementation for protecting institutional information systems; deficient internal control frameworks by management; insufficient security frameworks and standard operating procedures (SOPs) for documenting or overseeing these occurrences (National Crime Registrar, 2020: 12). The AGSA revealed further in the self-same report that there were 9,000 breaches of security suffered across the entire spectrum of government departments in a single year, which was emblematic of the rampant prevalence of improper security procedures (Palmer, 2016: 14). From an implementation point of view, the implication is that the departments ought to 'go back to basics' and put the correct procedures in place.

Over time, the researcher has also noted that the problem of departmental vulnerability to security breaches is largely a factor of non-implementation. For example, the State Security Agency has the Security Threat and Risk Assessment Framework, but government departments generally fail to implement the framework accordingly. The weakness in implementation may cause serious damages that might lead to significant financial losses, the confidentiality of sensitive information might be breached, it might create vulnerabilities in the critical assets of the departments and that may distract the core businesses of government (Govender, Sewpersa & Mahambane, 2015: 52). Some of the breaches entail technology equipment that have classified information, and that may damage the reputational image of departments, essential assets may become unavailable, privacy of personnel may be invaded, and service to the public cannot be delivered.

It is worth noting that government departments in some instances neither have asset insurance, nor the luxury of liberal budgets which could be spent to replace items that are stolen or damaged (Govender et al., 2015: 18). Consequently, they are compelled to develop and review their departmental strategies in ways that focus on combating and preventing corruption. In addition to monetary and non-monetary losses to the respective departments, they may also incur reputational damages and weakening of essential sections within the departments, create dissatisfaction, labour action, legal action, lack of confidence and risk damage to the overall image and reputation of government (Govender et al., 2015: 52).

Vulnerable departmental security programmes translate into cost-cutting by management and ineffective allocation of resources to the security divisions or sections of departments (Campbell-Young, 2016: 12). The STA should be implemented and then be monitored continuously for determining its effectiveness within the departments' security strategies, and for the purpose of accurately calculating estimated residual threats and risks (Whitman & Mattord, 2015: 277).

1.4 RATIONALE OF THE STUDY

The rationale of the research *per se* refers to the motivation or justification of the research as explained by the underlying reasons for its undertaking (Denscombe, 2014: 52; Henning, Gravett & Van Rensburg, 2013: 27). Furthermore, the rationale of research is also determined by, and located within the problem being researched; as well as the specific questions posed by the researcher in relation to *how* the researcher generated enthusiasm for a specific topic, and *why* the research is being conducted (Babbie, 2017: 36; Maree, 2007: 28). These propositions for the study rationale are in the same mould with the view by Creswell (2013: 130), to whom the problem statement appears to be synonymous with the rationale for the study. Babbie and Mouton (2012:

78) reflect that a clearly outlined research aim and well conducted research are observable in the research problem. According to Creswell (2014: 108), the problem statement is the main source of the study, which can facilitate exploration and provision of insight on the specific field that needs to be addressed and supported by credible evidence.

1.5 DELIMITATIONS/ DELINEATIONS OF THE STUDY

The delimitations/ delineations reflect the study's extent of narrowed focus or scope in relation to specific research variables, such as participants, sites, or type of research design (Creswell, 2012: 29; Henning et al., 2013: 34). In this regard, Kumar (2019: 47) concurs, adding further that those delimitations are reflective of boundaries or delineations determined by the researcher to restrict or confine the scope or 'reach' of the study; that is, what is beyond the control of the researcher or outside of the area of his/ her interest. Kumar (2019: 47) describes the purpose of delimitations in research thus:

- It guides the systematisation of the research path and related processes;
- It enables a pre-determination of the financial and expenditure implications of the research; and
- It lays out the study's epistemological, theoretical and practice-related boundaries or focus.

The present study is epistemologically confined to the concept of security threat assessment in government departments. Therefore, the research was only focused on exploring current efforts of government within the legislative, strategic and policy frameworks to assess the threats and risks that different national departments are facing. In this regard, provincial and local municipality level departments were not a primary focus due to the logistical and financial implications involved. Therefore, the researcher conducted the study only in Pretoria because it is geographically the place of residence of the researcher, which was cost-effective and saved time because all participants and national government departments are located in the capital city of the country (Pretoria). The researcher is aware that the incidents of theft, vandalism, sabotage, and cybercrime at National Key Points have increased in the past 10 years in strategic key points such as Parliament, Eskom, and Passenger Rail Agency of South Africa (PRASA) properties.

The study is confined to only the qualitative research design approach and a restricted sample of security managers in selected government departments. Furthermore, the study excluded personnel employed in non-management levels at the selected government departments, and those occupying the same management level at state-owned enterprises, non-profit organisations, and private-sector organisations.

1.6 AIM OF THE RESEARCH

Denscombe (2014: 49) and Flick (2014: 28) mention that the aim of research refers to the general intention or goal of the researcher in undertaking a study, as well as the reasons allocated for such intentions. Furthermore, the aim of research derives from both the research topic and research problem, and also provides a broader framework for the methods of collecting and analysing the data relevant to the study (Daniel, 2012: 16). The aim of this study is: To critically review the implementation of the security threat assessment by a selection of government Department in Gauteng.

It is on the basis of the above-stated aim that the researcher gained adequate knowledge and understanding concerning the existing counter-measures, their effectiveness, and reasons for their preference. The researcher's ultimate intention is to formulate an effective threat and risk assessment model and strategy that will assist in identifying threats and enabling responsible officers to monitor implementation, compliance and reassess residual threats.

1.7 RESEARCH OBJECTIVES

Research objectives are derived from a particular research aim, and articulate the specific activities and processes undertaken to further dissemble or reduce the aim to its most irreducible components (Bak, 2013: 29; Crossman, 2019: 12). The research objectives are then articulated thus:

- To explore and describe the scope of government's Security Threat and Risk Assessment (STA) framework guidelines,
- To explore and describe the role of other directorates when implementing the STA,
- To explore and describe the role of management in supporting security programmes,
- To explore and describe the process of appointing the Security Manager and the Security Committee, and their respective roles in threat assessment,
- To explore and describe the government departments' processes of anticipating and analysing the probabilities of loss and damage to State property,
- To determine whether or not current layers of security measures are adequate and capable of preventing threats before they occur; and
- To develop/ design an effective and implementable security threat assessment model or framework.

1.8 RESEARCH QUESTIONS

Maxwell (2013: 77) ascertains that research questions provide a precise picture of what is being studied, and warrants observation, measurement, and interrogation in order to illuminate broadly on the subject matter lodged or entailed in the research problem. The research questions also provide a focused direction on how the research objectives was approached for the overall study aim (Bak, 2013: 16). Each of the following research questions is linked sequentially to a corresponding research objective:

- What is the scope of government's Security Threat Assessment Framework (STAF) guidelines?
- What is the role of other directorates when implementing the STAF?
- What is the role of management in supporting the security programmes?
- Which processes are followed in appointing the security managers and in the selection of security committee members, and what role do they play in threat assessment?
- Which processes and procedures are in place in selected departments for anticipating and analysing probabilities of loss and damage to State property?
- What are current layers of security measures?
- Which possible solutions could be implemented to address the correct implementation of security threat assessment?

1.9 PURPOSE OF THE RESEARCH

It is the researcher's view that, whereas the research aim is mostly researcher-focused, the research purpose could be viewed as fundamentally research-based. The researcher-based proposition entails that the researcher himself/ herself introduces his/ her predetermined intentions and ideas to resolve issues he/ she has observed in relation to a particular situation (state of affairs) or phenomenon. It is in this regard that Thomas (2013: 6-7) accentuates the circumstance of the researcher (i.e., researcher-based proposition) as carrying some potential influence on the reasons for the study being conducted.

Therefore, the research-based proposition would entail that the ***already existing*** or ***prescribed*** research protocols become transcendental in directing or guiding the researcher's intentions insofar as synchronising the research aim and questions on the one hand, and the data acquisition and analysis on the other. It is in the latter regard that researchers wholly agree with the assertion by Babbie (2017: 16) and Denscombe (2014: 27), that the fundamental purpose of research is to enhance understanding and knowledge of an investigated phenomenon by means of exploration, description, and analysis of the various facets of the very phenomenon's manifestation.

Furthermore, Corbin and Strauss (2015: 19) and Kumar (2019: 1) declare that research is conducted in a methodical and systematic manner with the purpose of discovering the underlying issues and matters to sustain professional growth and integrity. That is to say, research allows for the development of existing knowledge on sensible scientific findings (Merriam & Tisdell, 2016: 27). Given all of the above-stated views and versions of the research purpose, the proposed study adopts an integration of both the researcher- and research-focused perspectives in its construction of the purpose of this study. Accordingly, the research purpose in the context of this qualitative study is to explore, describe, evaluate (i.e., analyse), develop good practice, and to empower the researched by uncovering the underlying truth of the research problem. The various attributes of the purpose of this research are discussed overleaf.

1.9.1 Exploration

Exploration entails the protracted search for more information or details in response to the "*what"* question concerning the characteristics or attributes of a situation or phenomenon in which the researcher is interested (Badenhorst, 2014: 19; McDowell, 2013: 37). The researcher first conducted a detailed literature search to explore various perspectives regarding the phenomenon of threat or risk assessment in the security environments. Such exploration provided informed understanding and theoretic knowledge in relation to government departments or officials' interpretation of policies and implementation of the STA in the interest of protecting the people (employees and citizens), and assets and information of the State (Smith & Brooks, 2013: 17). The research further explored various approaches for ensuring effective and efficient implementation of STA and define the role that Executive Management in the departments can play to support the Security Directorates.

The researcher complemented the theoretical (literature-based) exploration with empirical (primary) data obtained from the sampled participants by means of the interview mode of enquiry (Troy, 2020: 27; Warren & Karner, 2015: 18). Cast in this mould, the exploratory aspect of the research purpose also conforms to the methodology of the study as shown collectively in its philosophical worldview (paradigm) and qualitative research design approach (see Section 1.10).

1.9.2 Description

In both its literal (denotative) and methodological contexts, description involves the provision of further details (explanation) concerning a situation or phenomenon (Thanh

& Thanh, 2015: 26). According to Ritchie, Lewis, McNaughton and Ormston (2014: 55), the exploratory aspect of research precedes the descriptive aspect, but both aspects and processes should occur concurrently. As more information or details continue to be found through exploration, those details are explained in real-time to enhance their originality and undiluted authenticity. Therefore, whereas the exploratory aspect of the research purpose is concerned with the *who*, *what* and *when* questions, the descriptive domain then focuses mostly on the related *why* and *how* issues (Denscombe, 2014: 27).

During the interview stages of the research process and finalisation of the findings, the researcher explained the responses of the participants and provide more details from literature that support or disagree with the obtained responses (Crossman, 2019: 1; Denscombe, 2014: 27). These responses should express the wide range of descriptions of the STA environment and the implementation thereof; as well as determining whether the existing security measures are effective to protect the departments' critical infrastructure, and whether security managers are effectively implementing the counter-intelligence strategies to neutralise any potential or real threats.

1.9.3 Evaluation of the Current Situation

Evaluation entails a detailed scrutiny undertaken to facilitate the objective assessment and comparability of existing situations (Bordens & Abbott, 2014: 49; Denscombe, 2014: 27). The researcher reviewed and evaluated the existing security measures in the context of the departments' current implementation of the STA. The focus of such review was on determining the extent of challenges faced, level of vulnerabilities, strengths and weaknesses, and any ameliorative initiatives that may be in existence.

In the context of this study, the evaluation aspect is advantageous for its facilitation of comparing the current STAFs in various national, provincial, and local government departments with international best practices (South Africa, 1998: 12). Such a review trajectory further enabled the researcher's detailed scrutiny of prevailing challenges faced by the organs of the State, and *how* other countries were able to resolve challenges of such verisimilitude (Antinyan et al., 2016: 1). The collective effect of the exploration, description and evaluation of the security threat assessment and existing studies on the STA environments will enhance the development of a framework for improving the security threat assessment environment in government departments. The latter is consistent with the last research objective in Section 1.6 of this research.

1.9.4 Developing Good Practice

Developing good practice is the forte of research, and underlines the extent of contribution, particularly to the individuals and departments that are directly involved or affected by the outcomes of the particular research (Bertram & Christiansen, 2014: 74). The aspect of "good practice" particularises the form and nature of benefit or contribution in terms of the security managers' expected levels of understanding and knowledge pertinent to the field of security threat assessment and management for the better protection of State assets, people (staff and citizens), and information.

The researcher's foremost goal/ aim or concern is to resolve the problems outlined in the problem statement on the basis of credible and valid findings, conclusions and recommendations that will also contribute cogently to government departments to effectively and efficiently implement the STA. In that regard, the study reviewed the implementation of various international and local threat and risk assessment models to also identify any possible chasms in existing knowledge and experience.

Given the above, the intention of the researcher is to apply new knowledge and develop good practices that will provide effective and implementable guidelines and procedures for the STA at all levels of government. In addition, the information collected from this study will contribute to understanding by the security personnel and senior management of their crucial role in supporting security policies and procedures.

1.9.5 Empowerment of those Being Researched

Empowerment of those being researched implies the extent to which the study makes a practical contribution to the participants' improvement in the performance of their official duties in the realm of security risk or threat assessment. Generally, empowerment is about capacity, which is essentially developed or enhanced, amongst others, through knowledge, opportunities and skills (Adams, 2015: 21; Raacke & Raacke, 2012: 33).

The findings, conclusions, and recommendations will enhance understanding by security personnel, senior managers, and security policymakers in government departments of implementation of the STA, as well as world best practices in the sphere of detection, identification, and deterrence of internal and external threat and risk assessment during the execution of operations. Such knowledge and understanding will further develop the capacity of the relevant role players on salient factors such as aggressors' *modus operandi* and operational security (Pinnock, 2020: 12). Specific to this study, the role players, or those being researched and empowered refer to the executive/ senior management, security managers, counter-intelligence officers, and security officers.

1.10 DEFINITION OF KEY THEORETICAL CONCEPTS

Defining key theoretical concepts is helpful for accurate description and understanding of the study's foundational terms in order to distinguish their literal (denotative), contextual, scientific, and practice-related meanings and implications (Anderson, 2010; Daniel, 2012: 77). The following alphabetically listed terms/ concepts are also thematically associated with the study's core aspects as captured in the research topic.

1.10.1 Exploit

The term, 'exploit' generally implies making use of something for the purpose of gaining a benefit or an advantage (Taylor, 2008: 3). In this study, the security and threat assessment systems within government departments may be taken advantage of, by internal and/ or external threat agents aspiring to disrupt government services, destroy State assets or illegally gain access to secret or classified information to benefit themselves or their organisational principals (Whitman & Mattord, 2015, 12). Exposure or vulnerability of departments can also be exploited through documentary processes or digitally through the sophisticated software created by the aggressors.

1.10.2 Impact

Taylor et al. (2008: 3) describe 'impact' as an outcome or effect. In this study, impact denotes the effects, outcomes and implications of security incidences or breaches occurring due to non-implementation of, non-compliance to risk/ threat assessment frameworks provided for government departments in the STA.

1.10.3 Information Security

Govender (2018: 13) describes information security as any legal measures intended for protecting the integrity, safety, and confidentiality of information whose illegal availability could most likely harm the image and mandate of government departments. Taylor et al. (2008: 1) and Whitman and Mattord (2015: 10) also confirm that information security is intended to thwart the unauthorised disclosure or transmission of any protected information or assets stored or processed through the custody of the State through policy; education, training, and awareness; as well as technological means (Whitman & Mattord, 2015: 10).

1.10.4 Risk

Whitman and Mattord (2015: 13) define risk as the likelihood of harm, loss, or damage. In this study, the departments should reduce the likelihood of harm or loss in tandem with the amount and nature of damage that they can tolerate. Taylor (2008: 3) describes risk as the likelihood of the exploitation of vulnerability to a threat directed at a group or individual asset, and thereby causing harm to the departments.

1.10.5 Threat

Bayne (2020: 6) describes a threat as anything that can obstruct, destruct or interrupt a service or valued items. These threats can be separated into elements of people and non-living things. The process of analysing threats includes every element of risk that could possibly occur. Whitman and Mattord (2015: 13) allude that a threat is anything that signifies harm to assets and could be direct or indirect. The process of analysing threats could include a class of objects, people, and natural events. Whitman and Mattord (2015: 13) make an example of an information system that is not protected, and could be directly attacked by hackers, whereas an indirect threat example could relate to a severe storm that damages physical infrastructure and its contents. Govender (2018: 13) describes a threat to security as any individual or collective entities inspired to commit acts of crime, unlawful use of violence and intimidation, infiltrating or performing harmful acts that create a loss or damage to assets. In this study, threats relate to internally or externally induced circumstances intended to disrupt or cause damage to the normal functioning of the government department.

1.10.6 Threat Assessment

Black (2010: 471) describes threat assessment as a mechanism by security professionals, and law enforcement agencies to determine or measure the readiness of public and private institutions to proactively detect and deter possible risks. These threat assessment mechanisms are very distinct and may be in the form of complete written documents or digital or electronic systems and programmes that focus on averting threats before they occur. Allen (2016: 37) alludes to some important steps involved when conducting threat assessment. The first step is concerned with evaluating asset attraction and a wholesome risk assessment. The process is meant to provide value to the assets that are targeted and to discourage potential or actual aggressors. The assessment is conducted by the operators of that targeted assets. In this study, security officers could make use of these threat assessment procedures and processes when they perform their duties.

1.10.7 Vulnerability

Govender (2018: 13) describes vulnerability as any deficiency or weakness that exposes assets to exploitation by any aggressor. Meanwhile, Whitman and Mattord (2015: 13) describe vulnerability as a weakness or fault in security controls that could invite or attract attacks or damage to assets. An example of vulnerability could be a system port that is left unprotected, or a door that is not locked and attracts hackers to attack the computers of government departments.

1.11 RESEARCH METHODOLOGY

De Vaus (2013: 68) and Ravitch and Riggan (2012: 12) explain that research methodology is a foundational framework in terms of which the overall planning, design, and strategies pertinent to the research processes and procedures are managed. These processes integrate the research problem, aim, objectives, and questions on the one hand, as well as the collection, analysis and interpretation on the other. Such a continuum logically allocates a modicum of structure and coherence to the study and includes the philosophical worldview or paradigm of the study, the research approach, design and methods (Anderson, 2014: 52; Maxwell, 2013: 19).

1.11.1 Philosophical Worldview of the Study

A philosophical worldview or perspective premises mainly on a researcher's belief and value system, assumptions, speculations, abstract ideas, and perceptions of reality, nature, and knowledge (Anderson, 2014: 52; Mouton, 2014: 29). There are basically three fundamental or seminal philosophical worldviews (paradigms or perspectives) from which other offshoots are cognate (Bless, Higson-Smith & Sithole, 2014: 15; Noble & Heale, 2019: 12). These are: positivism, anti-positivism, and pragmatism. Whereas the proposed study predominantly adopts the anti-positivist philosophical perspective, the positivist and pragmatic perspectives are briefly referred to, for context.

1.11.1.1 The Positivist Worldview

The positivist worldview upholds that knowledge and understanding of the environment, the human condition, science, truth and reality is only possible through the application of objectivity (Creswell, 2014: 6). Such a perspective assumes that the researcher is able to observe, know and interpret situations truthfully only through detachment or being neutral from the situation being observed, studied or resolved. As such, the perspectives of the participants or those being studied are viewed as fraught with subjective experiences that will 'cloud' or conflate their judgement.

Therefore, statistically generated evidence (e.g., questionnaires) is viewed as the supreme form and source of truth and knowledge (Marshall & Rossman, 2016: 37; Raacke & Raacke, 2012: 29).

For the purpose of this study, the positivist paradigm was not deemed relevant since the study is neither predominantly statistical nor quantitatively inclined, except for the relatively minor instance of quantification of the prospective participants' demographic or bibliographic profiles.

1.11.1.2 Anti-Positivist World View

Anti-positivism entails a conglomerate of worldviews or philosophical perspectives that include constructionism, interpretivism, phenomenology, ethnography, and the ecological perspective (Mouton, 2014: 47; Welman, Kruger & Mitchell, 2012: 6). This motley of paradigms is cohesively linked or 'united' by the extent of their collective interstitiality in respect of "lived experience" as the foundational primary and most reliable and authentic account of the multiple realities of a phenomenon.

1.11.1.2.1 Constructionism and associated paradigmatic variants

The constructionist paradigm upholds that individual construct or develop experiences and information about themselves and their environment through social cooperation to which they are subjectively and emotionally or sentimentally attached (Tavakoli, 2012: 99). As such, the significant component of constructionism is its acknowledgment of socially developed or constructed realities and truths in specific settings and contexts, as opposed to the rigidity and objectivity of statistically inclined truth (Silverman, 2014: 26). The context- or setting-specific nature of constructionism immediately brings to fore, the effects and relevance of ecology (naturalistic environment or habitat) and ethnography (cultural factors) as influential factors in both the construction and development of truth-knowledge. Collectively, the constructivist-ecology-ethnography philosophical matrix/ milieu renders this philosophical paradigm relevant and applicable to this study.

In this research, the fundamental goal is to understand the environment in which the participants work, as well as their views about the state of the STA in respect of its implementation capacity in the detection and deterrence of actual and possible threats against the assets and information in the custodial care and protection of the State. Through the interviews, the researcher envisaged the construction and development of the findings and new knowledge on account of the sampled participants' experiences, perspectives, and perceptions concerning the (in)efficacy of threat or risk assessment in government departments as their primary ecological setting or habitat in which they have developed or even instituted certain organisational cultures as employees (David & Brydon-Miller, 2014: 26; SALII, 2018: 3).

1.11.1.2.2 Interpretivism and associated variant paradigms

In the qualitative research context, the interpretive worldview posits that relevant information sought for the purpose of addressing the research problem and its associated research questions is best obtainable from the world or lived experiences of the participants through their own words and discernment (Anderson, 2014: 55; Thanh & Thanh, 2015: 24). In this regard, the most distinguishable factor of the interpretivist perspective is that individuals and their translations, understanding, implications, and recognitions are viewed as the essential information sources (Mason, 2014: 56).

Furthermore, the interpretivist tradition views the individual’s impression of reality and the world as constituted by a series of subjective human connections, implications of perceptions, meetings and words (Anderson, 2014: 55). In addition, interpretivist researchers search for strategies that enable them to adequately understand the connection between individuals and their condition, and the part in making the social texture of which they are part (Thanh & Thanh, 2015: 260).

The interpretive perspective is linked to the phenomenological context in social research, based on the extent that the participants attach their own meanings to their own experiences in their own environment and in their own words. Accordingly, the interpretive paradigm and its associated phenomenological variant are deemed suitable for this research as they permit the researcher to view the world of government departments’ threat assessment capabilities through the discernments of the participants. The researcher then utilised the interview-based encounters with the participants to further develop better understanding of the meanings and reasons for their idiosyncratic interpretations of their world and its material circumstances and conditions.

1.11.1.3 Pragmatic World View

The term, ‘pragmatic’ is provenant from the Greek word 'prag-mein' and 'pragma', both of which mean ‘to do', and is also indistinguishable from 'practice' with the emphasis on what is/ has been done (results); in contrast with thought, intentions, or goals (Mouton, 2014: 8). According to Bless et al. (2015: 16), the logic about pragmatic reality of the world is not completely objective but is based on shared social information residing among communities. Denscombe (2014: 148) further clarifies that the pragmatic paradigm is viewed as a blended approach of strategies and techniques that recognises both subjective (qualitative) and objective (quantitative) methodologies. Accordingly, Denscombe (2014: 148) further intimates that pragmatism embraces the view that knowledge is not static and should be informed through practical or workable outcomes.

Denscombe (2014: 148) and Patil (2019: 11) allude further that research-based enquiry should test what works, since there is no absolute, single, best logical strategy and approach that is inherently able or qualified to deliver information through its own methodologies alone. Knowledge is viewed as temporary, what is known as truth today may not be viewed as such later. Therefore, pragmatism embraces the integration of quantitative and qualitative research for assorted information and methods for addressing the exploration, description and analysis of phenomena without the rigidity and confinement of a single approach or strategy (Hammond & Wellington, 2013: 126; Rees, 2016: 109).

The proposed study is predominantly reliant on participants' construction and interpretation of their own multiple realities and experiences, which find maximum expression through the qualitative research approach (Mouton, 2014: 37). In that regard, the pragmatic world view and its emphasis on mixed-methods research is viewed as not 'fit for purpose' in this study

1.11.2 Research Approach and Design

De Vaus (2013: 9) and Mouton (2014: 37) submit that the research design is a framework of planned strategies that guide and direct approaches for ensuring that data collected provides clear answers to the researcher's questions in response to the research problem. Creswell (2014: 3) adds further that the research approach and design is mostly defined and chosen according to the collective influence of the researcher's own experience, nature of the research topic and research problem; as well as the study's identified targeted audiences. Accordingly, the researchers' choice and decisions on the research design and its approach should consider their philosophical world view and assumptions, in conjunction with the specific research methodologies or procedures that translate their philosophical world view and assumptions into actionable outcomes (Hammond & Wellington, 2013: 126; Rees, 2016: 109).

Bless *et al*. (2013: 15) and De Vaus (2013: 9) confirm that qualitative, quantitative, and mixed-method approaches constitute three of the most commonly used research designs preferred by researchers. The choice of the current study's research design and approach was influenced by the constructivist-interpretivist philosophical world view as stated in Sub-section 1.10.1.2 of this research study. Therefore, this research adopted a qualitative research approach using an exploratory and evaluation research design. For functional purposes, the researcher conducted interviews with security managers in the SA government departments. Notwithstanding its qualitative trajectory, both the quantitative and mixed-methods approaches are briefly highlighted below for the purpose of contextualisation.

1.11.2.1 Qualitative Research Approach

The qualitative research approach focuses principally on the prosaic representation of information and data derived from the lived experiences of the participants as the most important providers or sources of such information (Bordens & Abbott, 2014: 231). Furthermore, the qualitative research approach is amenable to the constructivist-interpretive philosophical paradigm and its complete reliance on participant-centred construction and interpretation of reality.

As opposed to the inflexibility of quantitative approaches, the qualitative research approach is advantageous for its facilitation of onsite visits by the researcher in engagement with the participants (Bhat, 2020: 36). The proposed study adopted the qualitative research approach because of its allowance of the researcher to obtain information about threats and risks in government departments by interviewing relevant stake holders in those departments (Flick, 2014: 28; Yin, 2018: 8).

Furthermore, the researcher opted for the qualitative research approach for the flexibility with which the aspects exploration, description, and analysis are enabled in respect of the views of the participants concerning the state of security and threat assessment in government departments. The qualitative research approach is deemed appropriate due to its grounding on empiricism, which adopts a flexible, open, and unstructured approach to scientific investigation aimed at exploring diversity of information sources and methods (Kumar, 2019: 14; Yin, 2018: 9).

1.12 DATA COLLECTION

Data collection is the basic material that provides the basis from which researchers work (Durrheim, 2016: 51). It is in this context that data collection refers to the systematic process by which relevant information is obtained from different sources for its ultimate conversion into meaningful data relevant to addressing the research problem and its associated research questions (Dudovskiy, 2018: 19; Gravetter & Forzano, 2010: 27). Table 1.1 overleaf is indicative of the different data collection methods and procedures.

Table 1.1: Data collection methods, sources and procedures

Method	Sources	Procedure
Document review	Reports, newsletters, publications	Read all materials, documents and descriptive statistics related to the core research issue
Interviews	Primary participants	Audio recorded semi-structured interviews,
Observations	Secondary participants	Transcribed interviews of participants' interviews
Exit interviews	Observation of participants' interactions	Took notes and video-recorded the observations by informed consent

(Source: Researcher's own compilation from various sources)

In the context of this study, 4 (four) data collection methods were implemented, namely: literature review, documentary review, in-depth interviews, and personal experience of the researcher. Collectively, these methods reflect a triangulation of secondary and primary forms of data to be collected for the study (Warren & Karner, 2015: 17).

1.12.1 Literature Review

Wagner, Kawulich and Garner (2012: 271) report that a literature review is an analytical identification and interpretation of the consulted sources of information, received during the search for relevant materials addressing both the research topic and its related research problem. Corbin and Strauss (2015: 49) elaborate further that the review of literature should entail a systematic process in the search, identification, and processing of scholarship on the subject matter being researched. The review of literature is important in that it exposes the researcher to the most recent theoretical and methodological developments, current trends and practices, internationally and locally any shortcomings in the researched field; as well as lessons that could be learned to improve practice in the researched field (Walliman, 2015: 107).

The researcher conducted the literature review by gathering, assessing, and analysing relevant publications that relate to the research topic, the research problem, and the research questions. The researcher synthesised and summarised the sources by providing an overview of the primary opinions of each source (Thomas, 2013: 36). In addition to paraphrasing other studies, the researcher analysed the reviewed information by interpreting and discussing the importance of the findings in relation to the literature. The researcher also evaluated existing studies on threat and risk assessment by mentioning the strength and weaknesses as obtained from these sources in order to obtain more understanding on the state of security in government departments.

In his protracted literature review strategy, the researcher utilised the internet, Google Scholar, the University of South Africa (UNISA) library, relevant search engines and databases to access a range of sources such as dissertations, journals, theses, academic books, conference proceedings, and articles that relate to the research topic (Flick, 2014: 27). The researcher did not distance the study from other researchers but demonstrate further insight by comparing the findings of their studies. The researcher also collected information from international studies that address security threats and risks in both the public and private security environments. Prior to undertaking the study, the researcher read books in management security information, which are accessible to security managers and risk managers employed in government departments and entities.

Furthermore, the researcher delineated the study according to key concepts such as risk assessment, threat assessment, and others mentioned in Section 1.5 of this research. Such an orientation allowed the researcher to formulate various contexts and thematically coherent headings in order to develop a coherent structure of the study (Welman et al., 2012: 16), including international models that enhanced the researcher's intention to design the most suitable model for the South African context, which is consistent with the last research objective as articulated in Section 1.6.

1.12.2 Documentary Review

Documentary review entails the systematic search, identification and processing of written policy related texts and legal documents pertinent to the research topic (Dunn, 2013: 18; Tight, 2017: 44). Documentary sources are viewed as mainly non-academic in nature, but directly affects all levels of government, such as Section 209 of the Constitution of the Republic of South Africa (RSA), 1996, which provides for establishment and control of intelligence services in the Republic. The Constitution further makes provision for the limitations to individual rights under Section 36. The researcher investigated the Public Service Regulations, 2001 (Part VII, Section B (1)(F), which is a policy imperative for security checks and clearance or vetting of all employees only where the duties attached to their posts necessitate Such a course of action.

By its nature, the STA is a counter-intelligence tool, and the researcher has the responsibility to look at the National Strategic Intelligence Act 39 of 1994 as amended by Act 67 of 2002. In an amendment to the regulation affected in 2002, an obligation is placed on every employee to comply with the Minimum Information Security Standard (1996), also known as the MISS Document. Because of the physical nature of STA, the researcher further reviewed the Minimum Physical Security Standards (MPSS) which was published by the Government Sector Security Council (GSSC) in 2009 regarding parastatal facilities, government buildings, and national key points (South Africa, 1980: 1). The GSSC is a multi-sectoral committee chaired by the Ministry of Police and includes the National Intelligence Agency and representatives from various regulatory agencies and industry associations.

1.12.3 Interviews

Interviews are basically the encapsulation of focused dialogues or conversations between the researcher and the participants on specific aspects of the research problem (Guest, Namey & Mitchell, 2013: 4). Interviews could be semi-structured, structured, or unstructured; physical or virtual; face-to-face, telephonic or by email; individual or in focus groups (Creswell, 2014: 191). Unlike the quantitative data collection instruments such as questionnaires and surveys, interviews are advantageous in that they permit the researcher to obtain first-hand information in real-time (Durrheim & Painter, 2016: 111).

1.12.3.1 Semi-structured Interviews

The researcher compiled semi-structure qualitative questionnaire which provided direction to the participants and allowed them to express their experience whiles responding to the questions being asked (Anderson & Poole, 2014: 219). Moreover, Haven and Van Grootel (2019: 232) allude that semi-structured interviews allow for the participants to develop ideas and communicate freely with the researcher concerning the specific questions asked by the researcher. The approach is more flexible in terms of order of questions and how the subject matter unfolds during the interviews. Adams (2015: 493) mentions that semi-structured interviews are sublimely suited for a number of valuable assignments, especially when a number of the open-ended questions require follow-up questions.

Researchers should particularly consider utilising semi-structured interviews if they need to ask probing, open-ended questions on topics that the participants are not comfortable to answer in their peers’ presence (Flick, 2020: 82). The researcher should already have a topic for discussion during the planning and preparations for the interviews (Badenhorst, 2014: 43). Additionally, the researcher should have a choice of informants, authorisation, and the venue to conduct the interviews (Denscombe, 2011: 180-181).

Part of the STA is physical, which necessitates that those participants should be observed at their place of work to check their attitudes towards security of the departments. This allowed them to talk openly about issues of security threat assessment in an environment where they are comfortable. The researcher gathered information by means of a set of questionnaire checklist serving as the preferred instrument in this regard. By its nature, the STA may address information that is regarded as sensitive. The face-to-face approach was appropriate, where participants may not want to talk about such issues in a group situation (Dudovskiy, 2018: 37; Noble & Heale, 2019: 39).

In circumstance where a researcher is not able to conduct face-to-face interviews with the participants, telephone or internet-based interviews are deemed relevant. The researcher agrees with Anderson (2014: 219) that the current situation with the COVID-19 necessitates such interviews, with most professionals conducting their official meetings through platforms such as ZOOM, Microsoft-Teams, and Blue Jeans.

Web or internet-based interviews are easy to conduct, and are not time-consuming, they are cheaper compared to travelling, and they allow the researcher to access participants asynchronously for anyone in the world who has access to these platforms or even a cell phone (Anderson, 2014: 219; Leedy & Ormrod, 2014: 197). Researchers worldwide are now using the participant observation method (ethnography) to obtain personal and environmentally induced experiences of the participants. The researcher is a custodian of STA and works with a group of security specialists and security managers on day-to-day basis, which is a participant observation advantage for the researcher becoming a member of the group being studied in order to collect data and comprehend the culture and behaviour of the participants in their organisational habitat (Merriam & Tisdell, 2016: 105; Nobel & Heale, 2019: 47). During the participant observation process, the researcher assumes the role of a subjective participant and objective observer who does not interfere with the research proceedings.

On the other hand, in the event that COVID-19 restrictions became inhibitive to the participant observation method because of the number of participants conducting the STA, the researcher did not apply the mixed-methods approach in this study (Merriam & Tisdell, 2016: 105; Noble & Heale, 2019: 44). The latter approach is viewed as mitigating the weaknesses found in single-approach methods (McDowell, 2013: 5). This allowed the researcher to formulate a qualitative research questionnaire and email to the participants for their completion. However, the researcher acknowledges the possible shortcoming associated with sending the questions to the participants. For instance, in the event that the identified participants take long to respond, and some do not respond to the request at all after their initial consent to be involved in the study.

1.12.4 Personal Experience

Personal experience relates to the extent to which the researcher's own professional background and career experience collectively contribute to his/her involvement in the study (Dunn, 2013: 35; Gravetter & Forzano, 2010: 48). The researcher is a Counterintelligence Officer with an extensive professional background of training in Criminal and Corporate Investigation. The researcher is also a qualified Technical Surveillance Counter Measure (TSCM) Operator and Security Adviser through the State Security Agency: Security Management and Advisor Course 1/2019.

The researcher is also a member of African Association of Threat Assessment Professionals (AFATAP). The researcher joined the SAPS in 2002, and worked in various units within the organisation, including SAPS Training Academy, Crime Investigation, Crime Intelligence Unit, under Counterintelligence. The researcher is a Safety and Security, Sector Education & Training Authority (SASSETA) registered Assessor and Moderator, and he worked as Education Training Development Practitioner (ETDP) at SAPS Academy as an instructor from 2005 until 2009.

In 2010, the researcher obtained his National Diploma in Police through Tshwane University of Technology (TUT) and majored in Investigation and Policing. In 2013, the researcher enrolled and passed his Baccalaureus Technologiae degree with the University of South Africa. In 2014, the researcher was given an opportunity to enhance his knowledge in the Public Service Act by the Department of International Relations and Cooperation, as a Vetting Field Investigator at the level of Assistant Director and gained sufficient experience working directly within the SSA and aiding the South African Missions abroad. Part of his duties included assisting Operational Security and Mission Security Sections and conducting threat risk assessment nationally. During this period (2014 to 2019), the researcher has worked with different partner departments and has realised that most departments do not have an approved security policy and do not effectively implement the STA.

In 2019, the researcher graduated for his MTech degree in Forensic Investigations. In 2020, the researcher joined the City of Johannesburg Group Forensic and Investigation Services on the same level of Assistant Director, under the Minimum Information Security Standard Office. The researcher is currently responsible for providing security advice to the City of Johannesburg regarding protection of assets, people, and information in the custody of the city. In addition, the researcher conducts STA for City facilities, safety of councillors and their residences in consultation with the SAPS and SSA. On the whole, the researcher has realised that the issue of STA implementation is also existent in local government structures across the country.

1.13 POPULATION AND SAMPLING

A population in a research study relates to the larger group or wider pool from which the researcher's predetermined sampling components are collected, and on whose basis the findings was be generalised (Asiaman, Mensah & Oteng-Abayie, 2017: 1612; Durrheim & Painter, 2016: 133). Bless et al. (2015: 162) elaborate further and specify that the 'larger group' or 'wider pool' actually refers to the entire set of units or items, people or things, processes, systems, events, or activities in which the researcher is interested, for the purpose of determining specific attributes or units of analysis. Moreover, the specific attributes are then referred to as representative characteristics which provided direction on the process of including or excluding participants for any involvement in the study (Bak, 2013: 33).

Based on the above-cited propositions, the 'pool', population or larger group of this study consists of security managers; vetting managers; cybercrime managers; information security managers; physical security managers; and international practitioners or professionals in the security environment.

1.13.1 Target Population

Asiaman et al. (2017: 1612) and Daniel (2012: 57) state that the target population is the sub-group of participants possessing all, or most of the characteristics or qualities of significance that positively impact the goal of the research and assist in identification of the research problem's main variables and its resolution. Furthermore, the target population serves as the representative sub-group on account of the homogeneity (as opposed to heterogeneity) of characteristics that are already possessed by the larger group. Daniel (2012: 57) and Ritchie et al. (2014: 47) illuminate further that the target population is distinguishable by the following six attributes, which should be taken into consideration as they are vital elements to selecting a sample:

- Size of the population – an expansive population is helpful for common sense reason and to select sampling (permits in-depth investigation).
- Population homogeneity – it enhances sample selection when the characteristic of the population is similar.
- Population accessibility – when the researcher has easy access to the targeted population and there is an element of willingness, it benefits the research process and the study.
- Population spatial distribution – the location of the participants is one of the most important things to consider before the sampling commences, because it has financial implications, and it is time consuming.
- Population destructibility – expansive populace to permit guiding and deliver space for the most ideal chances for the researcher to conduct the sampling.
- Population continuous production – in the production processes and manufacturing, a sampling method is appropriate.

Based on the above-cited propositions by Daniel (2012: 57) and Ritchie et al. (2014: 47), Table 1.2 below provides a clearer context of the study's target population or sample size.

Table 1.2: Target population and related sampling variables

Target Population	Sample Size	Total
A: Security Managers	8	8
B: Vetting Managers	8	8
C: Cybercrime Managers	5	5
D: Information Security Managers	4	4
E: Physical Security Managers	5	5
Total	**30**	**30**

It is evident that the target population (N=30) is by far smaller in number compared to the study's population across all government departments throughout the country's nine provinces. However, small sample sizes are still helpful in situations where data saturation was the primary concern than the numerical involvement of prospective participants (Crouch & McKenzie, 2006: 18; Gravetter & Forzano, 2010: 46).

1.13.2 Sampling

Sampling is the deliberate or intentional selection of a smaller group of individuals, objects, or units to represent the larger pool or population from which they were selected (Anderson, 2014: 225). Meanwhile, Dudovskiy (2018: 28) adds further that sampling is a systematic process for selecting those population members who will eventually be included in the research study's empirical processes. It is not always possible to directly involve many or large populations of interest to the study's accomplishment of its overall goal or intentions (Warren & Karner, 2015: 64), which necessitates that appropriate sampling techniques or strategies should be devised for the singular purpose of obtaining suitable samples from the original or corresponding populations. Figure 1.1 (overleaf) is indicative of the sampled participants (target group) and sampling strategies used for their selection.

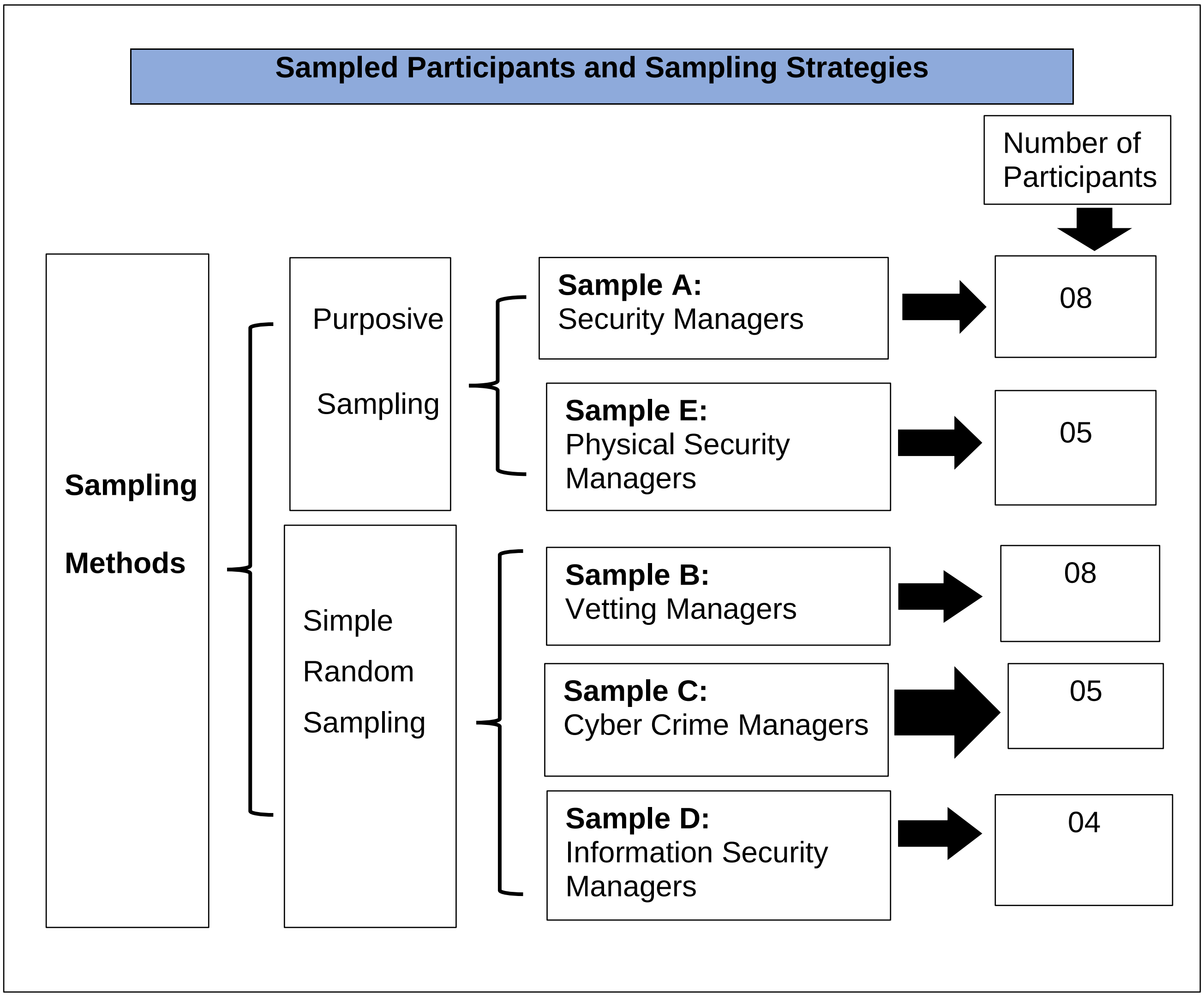

Sampled Participants and Sampling Strategies
Number of Participants
Sampling Methods
Purposive Sampling
Simple Random Sampling
Sample A: Security Managers
Sample E: Physical Security Managers
Sample B: Vetting Managers
Sample C: Cyber Crime Managers
Sample D: Information Security Managers
08
05
08
05
04

Figure1.1: Target population and methods of sampling used in the study

Whereas Table 1.2 highlights the different sub-groups or sample categories to be sampled, Figure 1.1 further indicates the different sampling methods that were utilised in the selection of the eventual target group.

1.13.2.1 Sampling Strategies/ Methods

Two sampling strategies or methods were used for selecting or sampling prospective participants in the study, namely: purposive/ judgemental sampling and simple random sampling. It is worth noting that the researcher was not personally involved in the selection of participants in order to eliminate any real or imagined considerations of bias, especially that the participants were known to him (Lanier & Briggs, 2014: 223; Thomas, 2013: 16).

1.13.2.1.1 Purposive/ Judgmental sampling

Purposive or judgemental sampling is an example of the non-probability type of sampling, in terms of which participants' chances of selection to the study are uncertain or not probable (Lanier & Briggs, 2014: 223). Other examples of non-probability sampling are convenience or availability sampling, quota sampling, cluster sampling, and snowball sampling (Walliman, 2015: 108). Purposive sampling is basically a sampling strategy in terms of which the researcher's own judgment is the primary standard for choosing potential participants (Dudovskiy, 2018; 49). Judgemental sampling is viewed as suitable for qualitative research, since it also allows the researcher to identify and determine the well experienced participants with rich information (Hennink, Hutter & Bailey, 2020: 27).

While exercising their own judgement, it is equally important that researchers should be optimally mindful of the potential for bias since they are familiar with what they require, and the participants may be known to them (Hennink et al., 2020: 27). In Section 1.12.4, the researcher has adequately demonstrated knowledge and experience in the investigated subject matter, as well as familiarity with all facets of the security threat assessment environment, including the most directly involved personnel in this regard. It is specifically against such background that the researcher ensured that he is not influenced by personal knowledge or professional relationships when selecting Security Managers who have completed the Basic Vetting Course, the State Security Agency's Security Management and Adviser Course, and have National Qualification Framework (NQF) 6. These participants were also expected to be fluent in communication and willing to express themselves convincingly and clearly with regard to security assessment issues.

Based on the above, and as indicated in Figure 1.1, the purposive sampling method was used for Sample A (the 8 (eight) security managers) and Sample E (the 5 (five) physical security managers).

1.13.2.1.2 Simple random sampling

Simple random sampling is an example of the probability type of sampling, according to which participants' chances or opportunities for involvement in the study are probable or certain (guaranteed) (Kumar, 2019; 117; Walliman, 2015: 119). Probability sampling examples include stratified random sampling and multi-stage sampling. The simple random sampling strategy itself derives from the theory of randomisation and its emphasis on the irregularity of occurrence of patterns in any situation (Almalki, 2016: 288; Burrel, 2017: 12). Therefore, the idea of "probability" and "random-ness" are central to implementation of this sampling strategy.

As shown in Figure 1.1, the simple random sampling technique was used for selecting participants in **Sample B** (the 8 (eight) vetting managers), **Sample C** (the 5 (five) cybercrime managers), and **Sample D** (the 4 (four) information security managers). Similar to the criteria applied for the selection of both Sample A and Sample E, the selection of participants in Sample B, C, and D was focusing on security managers who have completed the Basic Vetting Course, the SSA's Security Management and Adviser Course, and have National Qualification Framework (NQF) 6. These participants are also expected to be fluent in communication and willing to express themselves convincingly and clearly with regard to security assessment issues.

In essence, all participants were chosen because of their educational background and professional expertise that makes them the holders of the information required for the study. The participants' experience is very valuable for in-depth understanding of how the government departments implement the STA and other methods they have for neutralising potential threats. In addition to their experience, their availability and free-will participation in an insightful manner. In contrast, probabilistic or random sampling is used to make certain the generalizability of findings by minimising the possibility for bias in choice and impact of recognised and unknown variables (Burrel, 2017: 13; Denscombe, 2014: 48).

1.14 DATA ANALYSIS

Bryman (2012: 566), Durrheim and Painter (2016: 48) refer to data analysis as the systematic post-data gathering sorting, organising, and reducing data to a meaningful and manageable size, as well as looking for ways to reconstruct such data in order to interpret it when answering the research questions. According to Wagner et al. (2012: 269), data analysis also occurs when previously published information is compared to current data on the same topic. The accumulated information should be complete, rich, and broken down for findings based on careful analysis.

According to Bordens and Abbott (2014: 58) and Dudovskiy (2018: 47), qualitative data analysis could take any of the following five categories: content analysis, narrative analysis, discourse analysis framework analysis, and grounded theory analysis. Content analysis involves the processing of content information collected from an information source (Bordens & Abbott, 2014: 58). Narrative analysis involves the researcher's reconstruction of stories presented by participants, considering the context of every case and the exceptional experiences of each participant. On the other hand, discourse analysis involves the processing conversations, while, framework analysis involves familiarisation, framework identification, mapping, coding, charting, and interpretation. Meanwhile, grounded theory evolves with the analysis of qualitative data in a single case and formulating a theory. Additional cases could be examined to determine any contributions to development of a theory (Dudovskiy, 2018: 47). The following three-step analytic trajectory was pursued, as proposed by Dudovskiy (2018: 18-19):

Step 1: Code developing and application: Coding relates to the categorisation of data. A 'code' could be a phrase representing a main idea (theme) and are assigned significant titles. Non-quantifiable aspects such as behaviours, events, meanings, and activities can be coded in relation to the following three types:

- **open coding:** the preliminary organisation of unprocessed data for making sense, such as the transcription of the raw interview-based information for initial categorisation;
- **axial coding:** cross-referencing and linkage of categories of codes, such as synthesis and integration of recurrent themes emanating from various interview questions; and
- **selective coding:** cohesive formulation of the narrative by connecting the categories, such as finalisation of data from individual themes to global themes.

Step 2: Identifying themes, patterns, and relationships. As opposed to quantitative methods, there are no universally applicable relevant strategies to develop findings in qualitative records analysis. Analytical and fundamental questioning capabilities of the researcher establishes a massive position for information evaluation in qualitative studies.

Therefore, qualitative studies are not generally amenable to repeatability of identical results (Crossman, 2019: 7). However, there are methods of interpretation that can be used for common patterns, themes, and relationships within the participant responses in relation to codes detailed in the preceding stage (Dudovskiy, 2018: 19). More specifically, the most commonly used and effective methods of qualitative data interpretation include the following:

- Repeating words and phrases: involves the scanning of primary data for words and phrases that were frequently used by participants, including those considered emotional;
- Comparing primary and secondary sources: the empirical findings are compared with the reviewed literature findings for discussion of differences observed,
- Searching for missing information: those critical aspects not mentioned by participants should be discussed,
- Cross-triangulation: comparing the primary research results to phenomena from various perspectives and explaining their differences and similarities.

Step 3: Data summary: This closing stage is characterised by linking the findings of the research to the purpose and objectives of the self-same research study. The 'authorial voice' of the researcher should be prominent in articulating various points of views and contradictions from the findings.

The researcher methodically searched and arranged the interview responses, observation notes, or other non-textual materials that were accumulated to increase understanding of the researched phenomenon (Bless et al., 2014: 46). The researcher relied on extensive interaction with the security managers and expect to find unexpected and unanticipated information, which is not viable in the quantitative method. This approach assisted in analysing the security manager's perceptions on the implementation of the STA and their experiences in the field of counterintelligence and security services (Thoka, 2020: 27). The above-stated three-fold analytic trajectory assisted the researcher in discovering the perspectives and experiences of participants, as well as perceiving the constructions and meanings they apportion to difficulties associated with implementation of proper security measures in their departments.

1.15 METHODS TO ENSURE TRUSTWORTHINESS OF THE STUDY

Ary et. al. (2019: 442) proffer that trustworthiness is a demonstration of the precision, honesty, and validity of the findings. Trustworthiness is also described as the measure by which the study and its findings could be judged as having established trust and confidence within the research community (Creswell, 2014: 201). Basically, there are four qualitative measures in terms of which trustworthiness is established, namely: dependability, credibility, transferability, and confirmability (Walliman, 2015: 127). It is of further noting that these trustworthiness measures or criteria are most noticeable by any of the following 8 (eight) verification processes: triangulation, prolonged engagement, member checking, thick description (audit trailing), peer debriefing and clarification of biases (reflexivity/self-monitoring).

1.15.1 Credibility

According to Marshall and Rossman (2016: 47), credibility is reflective of legitimacy in qualitative research which indicates the extent of the study's believability as reflected by the concurrence between the findings and the conclusions reached by the researcher. The researcher ensured credibility through prolonged engagements with the participants after the formal interview sessions in order to understand their attitudes, perceptions, and other factors that influence the meaning they attach to their world view (i.e., the environment of security threat assessment). The researcher allowed the participants to share their knowledge and experiences in this regard (Elo et al., 2014: 3).

The researcher utilised triangulation to explore the evidence that would be collected from different sources in the field of security, and compare with literature sources (Asiaman *et al*., 2017: 1620). This entails drawing conclusions from multiple referents (Anderson & Poole, 2014: 36). It entails evidence from different sources, studies, and multiple perspectives from various researchers. The utilisation of triangulation allows researchers to distinguish between authentic and unverifiable information (Creswell, 2014: 201). This provided many perspectives about the topic, leading to acquisition of more realistic and denser information relating to the study findings.

1.15.2 Transferability

Babbie and Mouton (2011: 277) and Marshall and Rossman (2011: 252) define transferability as the extent to which the research process and its findings could be applied to other contexts or groups of participants. The researcher improved the study's transferability by making use of dense description of the findings.

It is rare for research studies to produce symmetrically identical results, despite the similarity of the problem/s (Alvy, 2016: 2). It is in that regard that the provision of thick or dense descriptions enable the readers to understand both the theoretical and empirical aspects of the study from its embryonic stages to its completion. Furthermore, such detailed descriptions (audit trails) are an enabling mechanism for future researchers to be familiar with all the steps in the research process for possible replication in the unique environment of their own research problems.

1.15.3 Dependability

Dependability depicts the consistency and stability of the results of the study over extended periods of time with different participants in contexts that are dissimilar to those under which the original study was conducted (Elo, Kaariainen, Kanste, Polkki, Utriainen, & Kyngas, 2014: 4). The researcher applied the dependability measure by means of the following:

- outlining and reviewing the precise processes of information gathering,
- asking similar questions for all the participants in the study,
- asking follow-up questions and providing clarity where questions are not clear,
- building a good relationship with the participants; and
- consistent coding and categorisation of themes (Elo et al., 2014: 5).

The researcher was reflexive throughout the research process and ensured that his own prejudices do not compromise the authentic views and perspectives of the participants (Adams, 2015: 24; Tavakoli, 2012: 29).

1.15.4 Confirmability

Confirmability is premised on the extent to which the findings of the study are affirmed or supported by others who were not directly involved in the study (Nayab, 2020: 19). It is on the basis of its confirmability that researchers and other practitioners in the same field of study could trust the findings as conforming to known research methodological protocols.

The researcher referred from previous studies that covered the area of risk and threat assessment for comparison of research findings. The researcher accurately documented the collected information from participants for their confirmation (peer debriefing) of the researcher’s interpretation. This method (peer debriefing) assisted in ensuring the accuracy of the responses provided by the participants (Aven, 2010: 355).

1.16 ETHICAL CONSIDERATIONS

Bertram and Christiansen (2014: 65) illuminate that ethics are meant for the moral, professional, and legally censored conduct, or behaviour of the researcher. Such conduct is essential, especially when the study includes humans, who have to be treated with honesty, dignity and respect (Gravetter & Forzano, 2010: 72). It is in the nature of research for researchers to comply with all ethical requirements, which ensures that the study being conducted is legally recognised and professionally accepted by various bodies and institutions (Bless et al., 2015: 29; Flick, 2011: 216) The researcher observed the following ethical protocols.

1.16.1 Institutional Review

The researcher complied with all ethical clearance protocols of the university as stipulated (UNISA, 2020: 1). The study cannot be recognised unless ethical clearance has been granted. The Department of International Relations and Corporations was consulted for permission to involve its personnel in the research. The SAPS and the Department of Public Service and Administration were formally consulted for permission to involve their respective security personnel in the study, as well as *in loco* observation and/or of security arrangements in selected government departments in Gauteng Province.

1.16.2 Non-maleficence

Participants were not harmed in any way as a result of their involvement in this research project. The researcher ensured that the interviews are conducted in a safe location at the participants' places of work since they were be held virtually. The researcher ensured that the participants are not harmed or intimidated by others who may disapprove of the current study (Bertram & Christiansen, 2014: 65).

1.16.3 Beneficence

The research should have the potential to benefit the well-being of others (Thomas, 2013: 17). In this regard, the researcher described the study's potential benefits, including those for participants and society as a whole. Upon completion, the researcher also offered to provide detailed information or a summary of the findings to the participants.

1.16.4 Autonomy

The participants should be free to participate voluntarily in the study (Warren & Karner, 2015: 27). Accordingly, the researcher did not compel the participants, nor make false promises or inducement to participate in the study. The researcher created a consent form that the participants signed to indicate that they were not compelled to participate in the study against their will, nor threatened with reprisals or penalties. These measures are also a recognition of the participants' legal and human rights insofar as making independent decisions is concerned. Such recognition was ensured with the researcher's announcement to the participant that they can withdraw from the study at any time. The researcher ensured that he exercises the principle of fidelity, in terms of which he faithfully keeps all these promises and agreements that he has made to the participants.

1.16.5 Justice

All interviewed participants were treated equally and indiscriminately regardless of their gender, disability, race, income level, or any other socio-economic consideration (Ritchie *et al*., 2014: 34). The researcher also informed the participants of their right to legal recourse in the event that they are of the view that the researcher has violated their human rights. Furthermore, the researcher disclosed the e-mail address of his academic supervisor for participants to report any unbecoming conduct on the part of the researcher, or further questions concerning the study,

1.16.6 Privacy, Confidentiality and Anonymity

The researcher ensured that the participants' involvement in the study is not made public, considering the high sensitivity of government information entailed in the research topic. The identity of the participants is protected with no reference to their names and places of work. In addition, pseudonyms were used, with no specific response attributed to any specific participant (Raacke & Raacke, 2012: 16). Additionally, all the information pertaining to the study, including the audio recorded statements of the participants, was digitally stored in a USB and the researcher's laptop which is protected by password only. Any unauthorised person is not afforded any form of access to such information, except the researcher's academic supervisor. Finally, all the digital and hard copies of the study will be chemically destroyed after a period of five years (Mills, Grimaila, Peterson & Butts, 2011: 37).

1.17 RESEARCH STRUCTURE

This proposed research is organised into seven chapters as indicated below.

Chapter 1: General Orientation

This chapter presents an introduction to the study in terms of the following key research variables: problem statement, the aim of the research and objectives, the value of the research, research demarcation, rationale of the study, as well as definition of the key theoretical concepts. This chapter further discusses the research design, research methods, sampling, population, data collection methods, data analysis, methods used to ensure trustworthiness, as well as the ethical considerations of the study.

Chapter 2: Literature Review

This chapter encompass a wide range of actions to identify, intervene and prevention of violent attacks on personnel in the work environment. The chapter also identify the type of offenders in the work environment in respect of threat assessment. It focuses on type of threats, as well as the difficulties associated with implementation of such psychologically informed activity in the context of counterintelligence. The chapter further discusses the role of other directorates, current mechanism of protection, and inclusion of mental health practitioners. The chapter also outlines in detail the implementation of the STA, and the role players involved. The chapter also reviews the relevant literature on the key concepts in order to provide a context for the research questions and aim of the study.

Chapter 3: Vulnerability Assessment

The chapter discusses the concept of vulnerability assessment and the importance of thereof. The chapter further focuses on the system components responsible for each vulnerability as well as the root cause of the vulnerability. The chapter further outlines the vulnerability assessment report and the rating method.

Chapter 4: Security Risk Assessment

This chapter focusses on security risk assessment as a combination of the likelihood of an event and its consequence. Risk assessment is limited to the meaning of work-related risk to uncertainty of financial loss, and the differences between actual and expected results, or the likelihood that loss will happen. This chapter further focuses on security breaches and the vulnerabilities to the core business of the departments. The chapter discussed the lack of security measures and exploitable weaknesses.

Chapter 5: Legal Mandate

This chapter proceeded with a discussion on the constitution, legislations, security policy development, procedures and proposed framework/practical guidelines. This chapter continues to discuss the international perspectives and experiences in terms of the use of implementation of STA and the difficulties thereof. This is followed by a discussion on the good practices in the field of counterintelligence and security studies.

Chapter 6: Research Findings, Recommendations, and Conclusions

This chapter presents the finalisation of the study with reference to the main findings, recommendations, and the researcher’s own concluding remarks.

CHAPTER 2
THREAT ASSESSMENT

2.1 INTRODUCTION

This chapter highlights threat assessment and distinguishes it from the associated task of risk assessment. The significant contribution of threat assessment is explained, as well as its potential in providing useful information relevant to identifying the weaknesses of the existing security measures in government departments. In this chapter, the researcher focuses also on insider and external threats, as well as the difficulties associated with implementing such psychologically informed activity in a counterintelligence context. In light of the identified security threats, the necessity and role of the STAF is reviewed.

Other security threat mitigation strategies such as avoidance, reduction, transference, and acceptance are also explored. These strategies include the necessity of linking threat assessment with threat management, along with the benefits and drawbacks of some of the many different approaches that can serve as a foundation and provide direction for the threat assessment and management processes (Patel & Bharadwaj, 2020: 1). Such investment in time and other resources could only be legitimised when there is an ample demonstration of accrued benefits (Bickley, 2017, 28). Accordingly, this chapter concludes with some observations regarding the evaluation of threats and management activities within the departments. This is because providing harm prevention services and demonstration of benefits could become a mountainous undertaking.

2.2 THE CONCEPT OF THREAT ASSESSMENT

A "threat" is perceived as a downside risk with negative repercussions (Sotic, Mitrovic & Rajic, 2014: 45). Risk itself is defined as a two-fold notion in international risk regulations and guidelines (Sotic et al., 2014: 45). This covers the possibility of both upside and downside risks, which could have a good or negative impact on achieving goals (Sotic et al., 2014: 45). Meanwhile, the term "opportunity" refers to the opposite of a risk. In practice, many departments struggle with adopting STA, which involves finding opportunities in the risk process, according to Hillson (2013: 1). Security managers find it difficult to identify a realistic opportunity, are unable to analyse or prioritise such an opportunity and identify available reaction alternatives, or how to manage the opportunities and alternatives themselves (Hillson, 2013: 1). They appear to have experienced different threats-related problems. In this regard, the study opines that the managers could be able to bring their practice in line with theory only if they believe risk management could address both opportunities and threats.

Government departments regard risk as a challenge, and are therefore unable to translate or convert it into an opportunity (Johansen & Rausand, 2014: 62). The COVID-19 pandemic presented a serious threat in the field of security, with the majority of security managers moving from contact security to digital security (Johansen & Rausand, 2014: 62). In addition, the most ominous threat to personnel security and the departments' integrity was the cessation of the vetting process by managers, which was intended to reduce the acceptance of multiple documents from the applicants. The pandemic provided the Vetting Field Units with the opportunity to implement "e-vetting", which allows the personnel to apply for vetting online. It is imperative to have competent security personnel to be able to identify threat sources (Mdluli, 2011: 7; Nkwana & Govender, 2017: 15).

The STA necessitates an understanding of threat sources, threat action, and how those sources can be used to exploit a vulnerability in a government departments' information asset (South Africa, 2016: 3). Although identifying threats in information systems is a critical stage in risk management, discussions concerning privacy and security have long been a major topic in the social sciences and in the public sphere (Onwubiko & Lenaghan, 2007: 4). There is a lack of a systematic investigation in identifying and categorising various sources of threats to information security and privacy (Bakhtiyari, Shahri & Ismail, 2012: 169). Based on the International Organization for Standardization (ISO/IEC27002), risk assessment is a critical strategy and identification of threats, and is one of the important stages in every Information Security framework. According to Govender (2012: 97), the discovered threats should be categorised according to their origin, motivation, and execution *modus operandi*. An analysis of the threat should also be carried out using the information provided.

It is recommended that the threat assessment should be supplemented with the analyses of both occurrences and vulnerabilities. It is important to base the decision on which targets need to be addressed on the assessment of the threat (Bakhtiyari et al., 2012: 170). It is further recommended that the security strategy should be utilised in the creation of a collective plan for the purpose of acquiring security information on the targets that have been identified. This strategy ought to be developed and administered by the security manager.

Mbowe, Zlotnikova, Msanjila and Oreku (2014: 166) acknowledge that it has been observed that the current threat assessment tools do not include information security policy for effective security management (i.e., confidentiality, integrity, and availability). This is because effective security management is dependent on the risk appetite and culture of the departments. The policy on information security is equally a tool that provides direction on how to manage and safeguard all departments' processes, including essential assets, infrastructure, and people working inside the departments. This guidance can be found in the form of an instrument called an information security policy. Critical assets, such as database servers, mails servers, web servers, and user smart devices, have been made more vulnerable to attack as a result of the absence of effective threat assessment frameworks in the local context (Mbowe et al., 2014: 167). This has led to an increase in both the risk of asset compromise and the probability that it will occur.

The need for an automated policy on information security mapped with a tool to assess threats is highly recommended against these threats (Mbowe et al., 2014: 173). Notwithstanding the government department’s size, an information security policy is required to integrate the security issues, controls, and the organisational commitment to protection of high-value assets and the information stored therein. Furthermore, such integration would enable the organisation/ government department’s strategic benchmarking capacity at any time interval, such as during security evaluation processes. In that regard, any organisational stakeholder would be able to automatically verify and check compliance to these security controls without relying on security expertise.

According to Deng (2015: 2), a threat is any act, event, entity, or phenomenon that is potentially harmful, and likely to cause a hazard or risk. Therefore, the term "threat assessment" refers to an evaluation of looming harm or danger posed by an individual, circumstance, group of individuals, or combination of circumstances. Allen (2016: 16) augments that a threat assessment/ evaluation encapsulates various activities intended to detect and analyse threat stimuli in situations where the threat has been detected. By its nature, the assessment/ evaluation of a threat or is foundational to regulatory decisions concerning the required or concomitant action proportional to the potential harm. According to Allen (2016: 16), threat assessment entails a comprehensive evaluation of asset attractiveness. It is then the mandate of the intelligence body to conduct threat assessments, which would consider the attractiveness of a target as well as terrorist capabilities and intent.

It is the function or duty of the STA to identify security weaknesses and review all existing security precautions for determining their efficacy, functionality, and practical relevance to the general security architecture (Smith & Brooks, 2013: 14). Following completion of the assessment, appropriate recommendations are then proposed to rectify any shortcomings, mitigate security hazards, and protect departmental assets. Preferably, such recommendations will serve as an indicator for businesses in their development of security plans commensurate with their overall business strategy. Govender (2018: 105) emphasises that each department faces a distinct threat. Therefore, it is important to consider specific hazards in each situation when the relevant security threat information has been obtained. Accordingly, individual security managers should learn to assess threats.

According to Vellani (2020: 34), accurate threat identification and confirmation is crucial for security decision makers, which enables them to prevent false-alarm reactions. However, no excellence in threat assessment can account for every potential eventuality. Criminals and terrorists and continuously invent new countermeasures. Cutting-edge counter-measures are becoming obsolete at an increasing pace in the contemporary technology-driven environment, and adversaries frequently follow suit (Vellani, 2020: 34). To keep abreast of the newest forms of threat intelligence, security decision makers are obliged to use the latest available technology-driven information sources in conjunction with the assessment report. When a possible form of danger is detected, management should support remedial action to either avoid or discourage the threat from occurring (Saleh et al., 2011: 18). Employees should be empowered to determine the goal and scope of the organisational risk assessment with the involvement of skilled professionals. Following the conclusion of the evaluation, management ought to then analyse the findings and act appropriately through the institutionalisation of a countermeasure strategy.

The STA is a single component of a comprehensive approach according to which government departments, personnel, and clients are positively and fairly supported in a comfortable environment where access points are established and physically protected (SAPS, 2011). The threat assessment process attempts to assess the likelihood that a person will commit "targeted violence”. In addition, the STA’s departmental procedures are aimed at evaluating and improving existing security measures in support of the security plan (Garcia, 2006: 24). To monitor the implementation of STA principles and procedures, security management should consider utilisation of a continuous improvement model. The researcher noted that government departments fail to implement in this phase, compared to the private sector's "value for money" approach. The government spends huge sums of money on improving security measures, but sparse monitoring of the implementation processes thereof.

Threat assessment typically includes a threat prevalence rate and the likelihood of future threat occurrence. Available historical reports are often most viable resources for creating the prediction of a threat occurrence (Dyer & Bowmans, 2021: 17). In the event that such resources are not available, other alternative sources should be opted for. That will help in developing a plan for future incidents. When a systematic approach to risk identification is used, the task of risk analysis becomes more manageable, and implementation of countermeasures becomes less complicated (Dyer & Bowmans, 2021: 17). Govender (2018: 116) argues that the incidents that occur in the departments are the results of security breaches, security practitioners' disciplinary breaches, and ineffective implementation of existing security policies and standard working procedures. The interpretation of threat is based on the incident, which may be defined as an adversary at the time of the occurrence, being the sum of intent and capability (Smith & Brooks, 2013: 12).

In the context of protection, many departments use the terms, 'threat' and 'risk assessment' within the services they offer (Harbach, Hettig, Weber & Smith, 2014: 33). However, there is confusion about its conceptualisation and methods. On the other hand, some believe that the threat and risk assessment are tools that are tailored to address the existing security measures for a specific client or department (Harbach et al., 2014: 33). However, the STA is not tailor-made, but rather developed to identify the type of threat existing at that time; as well as the methodologies for mitigating and reducing the risk of a present threat and identifying its magnitude. The STA is vital to practices of decision-making regarding asset allocation for control of risks or threats, and also fundamentally important in the initial processes of providing protective services.

It is the responsibility of security officials to understand the subtle distinction between a threat and a risk. Threats could originate from outside the departments or an aggressor who may cause harm to the system. Departments could receive threats linked to a break-in on the systems or hacks into the accounts of the department/s. The security system of the department is designed to prevent potential dangers from inflicting harm. According to Gritzalis, Iseppi, Mylonas and Stavrou (2020: 5), the STA is tasked with investigating threats to the departments’ systems and finding out which assaults are taking place in real-time or planned future attacks. The STA is able to collect information on attacks before they take place, which can help in identifying the scale of a threat, the level of danger it poses, and how it may affect the departments (Du Toit et al., 2002: 18). It is a more reactive approach to IT security, and it is a good option for organisations that need to know about real-time developments in their system, as well as approaches to address immediate concerns. This is an excellent alternative for enterprises to uncover digital dangers such as: programme vulnerabilities that may be used to inflict network attacks; the presence of malware or viruses; ongoing phishing campaigns that expose organisations to risks or breaches (Alshboul, 2010: 11). The inappropriate use of information can be uncovered through threat assessments, especially relevant to the financial and health sectors. Threat assessments are also helpful in detecting risks associated with employees, vendors, and individual customers (i.e., detecting anyone with malicious intent).

According to Sahoo (2021: 7), certain forms of assaults may be more effective against particular departments than they are against others. Targets include financial institutions, app developers, retail and technology organisations, to name a few examples. Since it is the data that is most frequently targeted, sensitive data is of utmost importance to departments working in areas such as finance and healthcare. Assessments of the potential risks posed by digital threats can be combined with applications and tools designed to track behaviour and cater to the requirements of the industry in question.

Sahoo (2021: 7) states that threat assessment is a sort of preventative activity that seeks to detect prospective violent actors before they act. This is done in an effort to prevent future acts of violence. Not only does this endeavour safeguard victims, but it also affords the opportunity to give assistance to a person who may in the future engage in violent behaviour Sahoo (2021: 7). In addition, a good danger assessment will minimise the harm to the departments' reputations and lessen the likelihood that they will be held liable for any miscalculations. Dhillon (2006) notes that threat assessment may be a newly established role in many departments or may have never been developed at all. Testing and exercise are required to validate policies and increase capability of staff members who are charged to carry out this vital role. This is necessary in order to develop security prevention capabilities.

The STA is an all-encompassing plan that identifies possible dangers and devises ways to neutralise them (Bayne, 2021: 11). This method uses a cross-functional team to conduct the evaluation of behavioural risks, which allows for the consideration of a number of different perspectives. Internal policy is the driving force behind threat assessment and pushes the threat assessment team to be alerted of warning indications, which increases their capacity to connect the dots (Bayne, 2021: 17-18). According to Diphoko (2021: 1), a threat is any situation that is likely to result in the manipulation, destruction, or disruption of any service or valued asset. During the analysis, every potential risk was taken into consideration. These dangers may be demarcated into two distinct categories: human and nonhuman, as exemplified in Table 2.1 below.

Table 2.1: Human and non-human categories of potential risks

Human	Non-Human
Hackers	Floods
Theft (electronically and physically)	Lightning strikes
Non-technical staff (financial/accounting)	Plumbing
Accidental	Viruses
Inadequately trained IT staff	Fire
Backup operators	Electrical
Technicians, Electricians	Air (dust)
	Heat control

(Source: Researcher's own compilation from various literature sources

According to Govender (2018: 70), security control measures have to be put in place in a manner that is congruent with the security policies and plans developed by the various departments. In the latter regard, judgments were taken to prioritise certain dangers that had not been handled in the past, or may not have been recognised as such. Threats need to be examined in connection with the business environment and the impact they will have on the department in order to assess them properly (Govender, 2018: 70). Both vulnerabilities and threats are intimately related, and may be rated using the same grading system, which is based on desire and capacity. It is also possible, for instance, that internal non-technical staff members may have little incentive to engage in harmful behaviour, but because of the degree of access they have on specific systems, they then have a high level of capacity.

On the other hand, a hacker would have a high level of motivation for hostile purpose in addition to the capability to cause damage or disrupt the business (Douglas, 2018: 1). Therefore, it is important to point out that motivation does not play any part in the prevalence of naturally occurring developments. A low grade could be allocated to a threat that has either very few capabilities or very little motivation. It is possible in that regard to award a high grade to threats that have both a high capacity and a strong motivation (Bayne, 2021: 18).

Govender (2018: 70) indicates that the measures to control security risks should be directed by the departments' security strategy in accordance with the departments' strategic objectives. The security policies and standard working procedures should communicate to the personnel in the departments, and the importance of security compliance should be emphasised. Non-compliance by disgruntled employees should be identified through these controls, and insider threat should be countered.

2.3 TYPES OF THREATS

There are mainly two major types of threats faced by government departments (Dlomo, 2004: 17). These are insider threats and external threats. Both threats are closely related, thus difficult to isolate from each other.

2.3.1 Insider Threat

The most significant security dangers nowadays are not caused by malevolent outsiders or malware (Alshboul, 2010: 11). Rather, they are caused by trusted malicious or irresponsible insiders who have access to critical data and systems. Most recent trends and challenges faced by departments, IT and security professionals' coping mechanisms against risky insiders, and preparations by departments to better protect their critical data and IT infrastructure have been noted to constitute critical concerns in a number of insider threat reports (Sharma, 2020: 7). For instance, the 2020 Insider Threat Report alludes that 68% of government departments believe that they are moderately to extremely vulnerable to insider attacks, while 68% of the departments believed that insider attacks were becoming more extant; and 53% of these departments were of the view that detecting insider attacks has become significantly to somewhat more difficult since migrating to the cloud-based information systems. Meanwhile, 63% of organisations viewed privileged IT users as posing the greatest form of insider security risk to organisations.

Insider threats are potentially the most significant obstacle that information technology (IT) and security professionals should overcome. In the present investigation, the term "insider threat" refers to "...intentionally disruptive, unethical, or illegal behaviour enacted by individuals with substantial internal access to the organisation's information assets" (Mills et al., 2011: 12). This definition articulates the nature of insider threat behaviour, and covers both current and previous workers, as well as contractors and other dependable business partners. Theft of intellectual property and confidential information by employees is and will continue to be one of the primary causes of financial and other losses, such as harm to individual or organisational reputation (Basdeo, 2017: 363). The recent Wikileaks documents in which large amounts of sensitive material were leaked by a reliable insider and finally published on an open website, has resulted in analysing the security behaviour of end users. The March 2005 issue of Computers & Security has shamed the United States of America (USA) and other countries in terms of worst-case insider threat scenarios.

Mills et al. (2011: 12) add that the ‘wicked’ problem of insider threat is multifaceted because of a variety of contributory elements that either worsens it or engenders new problems. It is sometimes impossible to differentiate between regular behaviour and the malicious actions of an insider, making it difficult to even identify assaults before the harm has been inflicted. Most insider assaults, on the other hand, are organised, and there is a window of opportunity within which individuals may act and either stop the attack entirely or, at the very least, reduce the amount of damage that it causes (Mbuvi, 2011; 12). On the other hand, the focus placed on lean management causes supervisors to have less time and miss possible warning signs.

Insiders provide a substantial risk since they are familiar with the information and/or systems of their employers and have access to such systems and/or information (Mdluli, 2011: 33). They do this daily in a way that is completely legal and circumvents both physical and electronic security measures. A malevolent insider does not conform to any demographic profile. They could be male or female, married or single, young or elderly, and members of any number of different ethnic groups. Furthermore, a discovery has been made of several identifying characteristics of insiders and the crimes they commit, which may be exploited to build measures for mitigating their effects (Campbell-Young, 2016: 1).

Garg (2020: 2) define an insider threat as any potential harm posed by any currently or previously authorised person/s with access to information networks, facilities, resources, or relevant people; and who intentionally or otherwise commits, acts against, or violates the law or policy and results in, or might result in, harm through degradation or loss of government or organisational information, capabilities, or resources; or detrimental acts, including physical injury to others. Grama (2011:14) further declares that an insider threat should not come as a surprise if the departments have not defined an insider danger. This is due to the fact that historically, only the external risks have been emphasized. Regrettably, very few departments possess a clear, internal working definition of their own. The South African government is prone to utilising contractors and bringing in outside talent to fill technical and scientific roles.

An employee, contractor, or vendor who performs an act of malice, complacency, or ignorance utilising his or her trusted and validated access might be considered an insider in the organisation. The identification of a potential risk inside the department is the first step in the process of developing a programme, as well as its structure and scope. Gruyter (2021: 3) contends that negligence, lack of security awareness, and distraction constitute the most common causes of unintentional insider threats. On the other hand, malicious insider threat is caused by factors such as willingly, intentionally, and/or nefariously engaging in activity for financial or personal gain in this $200 billion dollar brokering industry in which data symbolises power, money, and influence.

According to Harbach et al. (2014: 11), a negative work event such as a termination, demotion, or disagreement with a supervisor, preceded a significant percentage of insider threat cases, and 59 % who leave departments voluntarily or involuntarily confirmed that they took sensitive information with them. Based on the researcher’s experience and observation, employees generate voluminous sensitive data in their official capacity on behalf of their departments, but when they discharge, there are no processes of declaration to ensure that no organisational or classified data are stolen. According to Harbach et al. (2014: 11), the typical enablers of insider IT sabotage are the technical users with privileged access, such as system administrators, programmers, and database administrators. The foremost motivation in these crimes is usually linked to retaliation for a negative workplace event. These crimes are frequently planned during the period of employment, but are carried out after termination of the employer-employee contractual association.

In the last thirty years or so, the tactics of the insiders have evolved from stealing ordinary paper files to exfiltrating digital data (Hlongwane, 2013: 1). The researcher concurs with Hlongwane (2013: 1) that in era of globalisation and social media, employees exchange sensitive information on social platforms using technology-driven methods and approaches. The development of new security technologies is ongoing in order to counteract newly discovered security flaws and methods, but there is one type of attack that cannot be neutralized by merely putting in place more advanced tools and procedures. The most significant dangers to information security in the modern world are not the work of malevolent actors, sophisticated persistent threats, or malicious software, which originate from the individual. The researcher agrees with Antinyan et al. (2016) that working remotely is the most dominant trend in the contemporary era. More team members work from home, more devices are connected to their network, and new technologies and tools are being developed to assist at-home offices to functioning properly. Based on the latter, the researcher believes that this trend will continue into the foreseeable future.

Thompson (2019: 17) argues that the threat posed by insiders is a security risk originating from the targeted departments, which does not presuppose that the actor is a current employee or officer of the departments. The insider could be a consultant, a former employee, a service provider, or a member of the board of directors. On the other hand, an insider threat could be internally orchestrated by negligent or malicious departmental insiders, current or former employees, service providers, stakeholders, or third-party vendors who have inside/ internal knowledge of sensitive data, cybersecurity practices, and computer systems (Business Insider SA, 2020). Sabotage of security measures, fraud, theft of intellectual property, confidential or commercially valuable information and trade secrets, or misconfiguration that results in data leaks may all be part of the threat. The next sub-section below discusses the different types of insider threats and their nature.

2.3.1.1 Non-responders

A small percentage of employees are not interested in attending security workshops and awareness programmes. Most of these employees are usually the people who compromise the security of departments (Thompson, 2019: 12). The employees who have a history of non-compliance or harming the security are likely to repeat the feat on the basis of consistent patterns.

2.3.1.2 Inadvertent insiders

Failure to comply with security measures is the most common form of insider threats, and has high financial implications to the departments (CERT, 2014). These are employees who are not willing to comply with standard operation procedures and the security policies of the departments but compromise the security due to isolated errors. The most common occurrences by the insider threat are employees who store the intellectual property on their personal devices.

2.3.1.3 Collusion from within

Insider collaboration with harmful external threat actors is an uncommon occurrence, and poses a substantial risk because of the increase in the number of times that hackers try to recruit employees through the dark web. According to research conducted by the Community Emergency Response Team (CERT, 2014), the trend by insiders and outsiders working together to commit security breaches was responsible for 16.75% of all incidents caused by insiders.

2.3.1.4 Persistently malevolent insiders

This category of insider threat most frequently engages in data exfiltration or other forms of criminal activity, such as the installation of malware with the intention of obtaining monetary advantage (CERT, 2014). Research conducted by Gartner on the topic of criminal insider risks discovered that individuals looking to supplement their income constitute about 62 percent of insiders with malevolent intent.

2.3.1.5 Disgruntled employees

Employees who are dissatisfied with their jobs have the potential to steal intellectual property, disrupt security tools, and violate data security standards (Duff, 2010: 12). Such workers tend to exhibit predictable patterns of behaviour, which is possibly identifiable through behaviour analytics (Duff, 2010: 12). For instance, when they have been dismissed, give notice of employment termination, or dismissed before their information access is withdrawn, they can start looking at sensitive data sources.

2.3.1.6 A mole

A mole is an impostor who is an outsider, yet has managed to obtain access into the organisation (David & Brydon-Miller, 2014: 7). This refers to an individual from outside the company who masquerades as an employee or partner of the company. According to David and Brydon-Miller (2014: 8), insider threats typically manifest themselves in the following three-fold dimensions:

- Malicious insiders are the most uncommon, but pose the greatest threat to the organisation because of their access to confidential information. It is extremely detrimental to have managers with privileged identities, and the most expensive security breaches are those that are caused by malevolent attacks.
- Insiders who have been manipulated can be "tricked" into disclosing critical information or passwords by using social engineering techniques.
- Unscrupulous employees could accidentally delete or change crucial data by pressing the wrong key on their keyboard.

There is also the possibility that privileged or regular staff having access to sensitive information could be the source of an insider threat. Personnel frequently have unrestricted access to a range of crucial systems and are capable of carrying out nearly any task. People of all different sorts frequently have more entitlements than they need in their present key performance area, which results in an elevated risk that could have been completely avoided. (David & Brydon-Miller, 2014: 7-8). Some of these insider threats are not intentionally compromising the security of the departments, but they lack knowledge and unintentionally put the security at risk. Some of the employees start to panic now during the COVID-19, when they are working from home and computers anti-viruses need to be updated, and the storages are full. The personnel are using their personal computers and hard drives to back up the official data.

The likelihood that an insider will utilise their official authority to access the information or an institutional memory to cause harm to that departments is referred to as an insider threat (Ramluckan, 2019: 1). Such harm could include malicious, unintended, or careless acts that endanger the departments' data, personnel, or facilities' integrity, confidentiality, and avail ability. This commonly used definition could be more appropriate and adaptable to the requirements of outside stakeholders and DHS customers. In the parlance of the Cyber and Infrastructure Security Agency (CISA), an insider could (intentionally or unintentionally) use his or her authorised access to induce harm to the Department of Defence’s mission, equipment, resources, facilities, personnel, and information networks, or systems. Such a threat has the potential to damage to the department as a result of the following behaviours exhibited by insiders: unauthorised information disclosure, workplace violence, terrorism, corruption, including participation in transnational organised crime, sabotage, intentional or unintentional loss or degradation of departmental resources or capabilities, and espionage (Ramluckan, 2019).

Managing the human element is the most difficult aspect of managing insider threats (Defence Science and Technology Organisation, 2010: 12). Naturally, employees would like to earn the trust of their employers, and they become distracted when the departments employ new strict security measures that would prevent them from having access to information, they previously had access to. For IT administrators, having access to the departments' critical information is a form of status, and being prevented to access such information can be met with resistance. Many security breaches committed by insiders are unnoticed. As such, departments are concerned about the reputational image and would prefer to keep these breaches internally (Garaba, 2012: 33). However, numerous highly damaging insider breaches have been revealed. Table 2.2 below is an illustration of some of the well-known insider breaches in the United States.

Table 2.2: Examples of well-known insider breaches in the United States

National Security Agency	San Francisco	Motorola
During the time that he was employed as a **contractor for the National Security Agency (NSA) by Booz Allen Hamilton, Edward Snowden leaked highly** sensitive documents to members of the media using software applications known as "Prism" and "Boundless Informant." The documents provided by Snowden disclosed specifics on the storing and processing of communications by the NSA, such as phone calls and emails.	An employee with a grudge against the city of San Francisco was responsible for locking the city out of its own FiberWAN network, which had sensitive data such as police records. Alarmingly, emails and payroll checks could not be issued because they were rendered inaccessible. In an effort that was ultimately fruitless, the city spent more than one million dollars trying to connect to the network.	Hanjuan Jin, a software engineer who worked for Motorola for nine years, was apprehended by officials from the United States Customs and Border Protection as he attempted to board a plane to Beijing with $30,000 in cash and over 1,000 documents labelled "confidential and proprietary information." Together, these items represented between $10 and $15 million in trade secrets. A federal court in the United States convicted Jin guilty of stealing trade secrets and sentenced him to four years in prison for his crime.

Source: Miller & Maxim (2015: 6)

Collaboration between malicious insiders can lead to a larger attack by accessing organisational assets (Alshboul, 2010: 2). In the realm of theory, several actors could conduct reconnaissance from within the "need-to-know" aspect of their job responsibilities to commit intellectual property theft or fraud. As a result, these malicious actors may be able to avoid detection, posing a real risk to the departments through collusion. Collusion relates to occurrences wherein insiders collaborate to attack a company or organisation, rather than utilising social engineering for the manipulation of other employees (Alshboul, 2010: 2).

The insiders have their own method to communicate, known as a communication channel, which they use between one or more people involved in the incident while it is being planned or executed (Alshboul, 2010: 2). This communication takes place between those who are knowingly engaging in or participating in the insider incident: insiders, an insider and an outsider, or the insider and various third parties. Communication between parties does not have to include the transmission of sensitive information. The insider and co-conspirators could simply be plotting a hostile act. An exfiltration channel is not a communication channel for our purposes unless stolen data is sent between two people. For example, an insider stealing data by emailing it to themselves is not a communication--it is purely exfiltration. In contrast, an insider stealing data by sending it to someone else is a communication as well as an exfiltration (Blanchard et al., 2020).

According to Broder and Tucker (2012), it is unsurprising that the most targeted departments were occupied by the most common asset owners across all insider threat case types, including fraud, IP theft, and sabotage. Therefore, the assets of the clients are not always targeted. It has been observed that there are few targeted assets belonging to employees, third parties, or others. Figure 2.1 below depicts the owners and types of assets targeted in insider threat incidents.

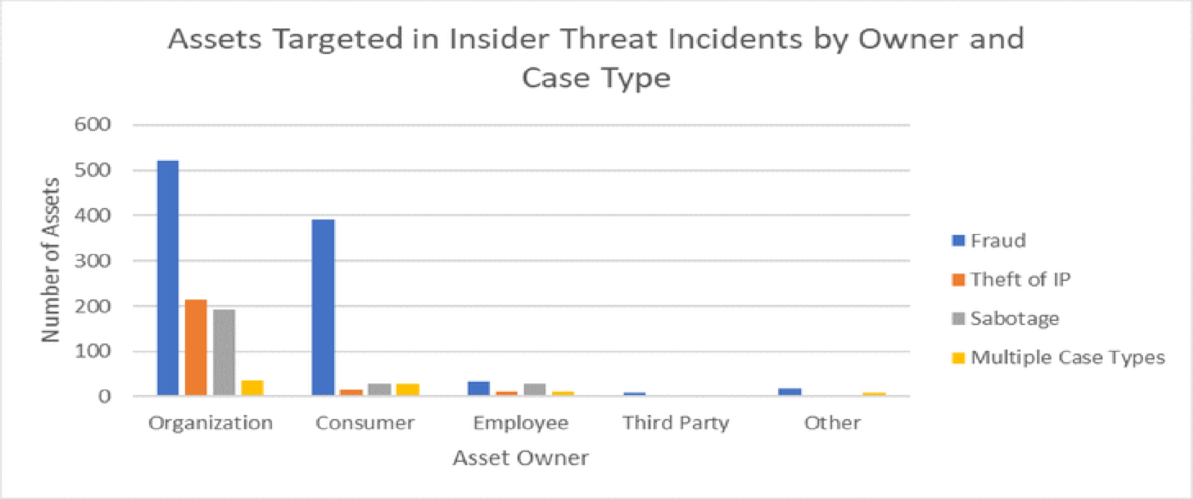


Figure 2.1: The CERT insider threat incidents by owner and case types

Fraud incidents, which account for many corpus incidents, were linked to most targeted assets owned mostly by organisations and by consumers to a lesser extent (Association of Certified Fraud Examiners. 2014).

Chou (2013: 79) states that an insider threat could be posed by a single employee, contractor, or vendor who, because of their access to information, materials, people, or facilities, has the potential to harm a department’s due to ignorance, complacency, or malice.

Table 2.3: Examples of insider threats

Data Exfiltration	Fraud	IT Sabotage	Workplace Violence	Espionage
Sensitive information developed or supported by the departments may be stolen by those looking to extract confidential data.	Insiders who have access to the departments' data may be able to facilitate financial fraud or collusion.	Insider actions, such as malicious sabotage of IT systems and data, can put critical infrastructure at risk.	Employees may face violence or the threat of violence from a colleague or someone who targets their departments.	The departments' role within the government raises the prospect of nation-state espionage.

Source: Chou (2013)

The insider threat originates from inside the departments, and different counterintelligence methods (e.g., vetting process) could be used effective for identifying the aggressors (Mdluli, 2011: 7). The researcher discussed the acts of corruption from employees and sabotage as common threats by the inside aggressors. Most of these employees have not gone through the vetting process and they are occupying critical position which give them access to sensitive information.

2.3.2 External Threats

According to current security thinking, external threats could be military, political, social, economic and environmental (Mohlabeng, 2020: 1). Obviously, the state, people, geographical areas, and the global community are now all referent objects of national security.

To analyse the aforementioned, it is now exceedingly problematic to differentiate between internal and external security concerns. The reason for such difficulty is that, as a result of the influence of globalisation, domestic or internal hazards have become internationalised, while international or exterior threats become domesticated (Mohlabeng, 2020: 1). However, in recent years, the migration problem has proven to be a huge external danger to South African government departments and the country as a whole. Mohlabeng (2020: 1) claimed that the view of immigration as a danger to security has arisen alongside the significant growth in the number of immigrants globally. Undocumented immigrants present a threat to national security in South Africa (Mbuvi, 2011: 17).

Furthermore, the Mozambican problem of an Islamic State (ISS) insurgency and attempts to capture a portion of the country's northern portions, offers a severe threat to South Africa, with government departments and State institutions being specific targets. It is the responsibility of government departments, in partnership with security organs, to be always alert to foreign dangers (Mohlabeng, 2020: 1).

Illegal immigration has been related to additional dangers such as criminality, which jeopardizes the operations of the majority of government departments. Officially, there is a causal association between migration and crime, according to the Southern African Migration Project (2016: 1). Crime statistics for police operations often include arrests for "illegal aliens" alongside arrests for armed robbery, carjackings, and rape (Southern African Migration Project, 2016: 1). If these crimes are not thoroughly investigated, the government may fail to identify the scope of the problem and develop plans to combat it.

2.4 CYBERSECURITY THREATS

Nowadays, almost all businesses conduct their transactions online and share massive volumes of data over the internet. As cybersecurity risks continue to plague government organisations, there are major risk factors that should be carefully monitored (Bishop, 2003: 68). This is due to the persistence of cyber risks as an increasing number of organisations and individuals recognise the usefulness of the internet. As a result of this growing internet dependence, cybersecurity concerns such as identity theft (phishing), harmful programmes (malware), and data encryption (ransomware) have emerged (Douglas, 2018: 2). In its Financial Stability Report published on 28 November 2021, the South African Reserve Bank (SARB) highlighted cyber risk as one of the banking sector’s primary threats. The SARB further warned that cyber-attacks could directly affect financial institutions through financial losses, additional to the indirectly incurred costs such as reputational harm to the banking industry. It is worth stating that cybercrime cost is difficult to calculate due to South Africa’s lack of any regulatory mechanism requiring transparency (Isa, 2020).

Hackers make use of a wide array of strategies due to the fact that they are constantly developing new strategies that are supported by innovative technology. According to Fruhlinger (2019: 7), phishing and malware attacks are common methods that hackers use to gain access to information without being required to send direct queries to the victim (Fruhlinger, 2019: 7). The lack of cybersecurity information on the part of consumers, hackers are successful in their attempts. This lack of understanding permits backdoor flaws that expose various enterprises (Fruhlinger, 2019: 3). Phishing, virus, and ransomware attacks continue to focus on public organisations since they are considered "soft targets" in the cyber world (Douglas, 2018: 1). Each of these threats will be examined in greater depth in the following paragraphs.

2.4.1 Phishing

Phishing is the use of a 'friendly' email message to deceive the receiver into disclosing more of the information than usual under normal circumstances, which benefits the hacker (Jagatic, Johnson, Jakobsson & Menczer, 2007: 95). Increasingly, phishing attacks are becoming more common in online cybercrime, with the goal of fraudulently gaining access to sensitive data. Attackers target government organisations because they lack effective security procedures and are considered easy targets (Hutton, 2017: 2). Emails encouraging victims to log on to phony websites and disclose private information tempt the victims of these assaults (Isnaini, & Solikhatin) (2020: 80). According to Lee (2014: 31), eliminating phishing websites timeously has proved a futile endeavour due to cross-border jurisdictions.

Many phishing attempts employ the social engineering strategy since personal information is the most likely to provide the intended consequences (Sutherland, 2017: 85). According to Nkwana and Govender (2017: 14), most IT users rely on the internet to read emails and conduct transactions, putting them exposed to phishing attempts. According to a Hutton (2017: 1) survey, 82 percent of public sector employees open email attachments without first reading the email's text. Despite being informed about sophisticated phishing attempts as part of their security training, they continue to fall victim to them.

2.4.2 Malware

Hackers are also using different methods to create ‘malicious tools in order to exploit susceptible individuals (Patrick et al., 2016: 76). These dangerous weapons take the form of viruses or worms that include pre-programmed instructions (Patrick et al., 2016: 75). Because public sector personnel execute the majority of their everyday duties online, they may find up viewing sites that are packed with malicious tools, compromising the systems of public sector organisations (Douglas, 2018: 4). Many public-sector organisations are at a disadvantage in dealing with such cybersecurity concerns due to a lack of cybersecurity expertise (Patrick et al., 2016: 76).

2.4.3 Ransomware

In recent years, there has been a rise in malware assaults, including ransomware. Ransomware attacks compromise a user's system by exploiting insecure or unpatched systems. Following that, they encrypt all data, including the hard disk, and demand a ransom in exchange for the decryption key (Luo, 2017: 195). Ransomware continues to be a major worry for public sector organisations, as recent assaults in South African government departments demonstrate the need of patch management compliance and robust network security policies that ought to be in place and followed (Patrick *et al*., 2016: 76).

2.5 IMPACT OF CYBERSECURITY THREATS ON THE PUBLIC SECTOR

The information technology systems of the Department of Justice and Constitutional Development (DOJ & CD) were breached in September of 2021, which hampered the department's capacity to make payments for child support (Diphoko, 2021: 1). The gravity of cyberattacks is demonstrated by this incident and the impact it had on businesses that are part of the public sector. According to Patrick et al. (2016: 76), a lack of skills and knowledge about cybersecurity among IT users makes South African government departments more susceptible to cyberattacks than private sector organisations. Another factor that puts companies in the public sector at risk is the significant lack of skills, in addition to the amount of time that is necessary to build up a substantial pool of skilled employees (Masse, O'Neil & Rollins, 2007: 2). This accounts for time spent learning in academic settings as well as time spent obtaining professional experience (Nkwana & Govender, 2017: 14). It is possible that initiatives led by the government to build specialized centres of knowledge or training facilities for developing cybersecurity skills could contribute substantially to filling the skills gap in the government departments.

2.6 CORE BUSINESS ANALYSIS AND IDENTIFICATION OF CRITICAL INFRASTRUCTURE

Govender et al. (2015: 32) indicate that every business, no matter how large, small, or sole proprietorship, owns some property or assets. As a result, the departments face the risk of malicious property damage caused by housebreaking, theft, arson, or sabotage. The assets of the departments can be both tangible and intangible. A tangible asset is something that can be seen, such as a car, and an example of an intangible asset is an departments' good name, which cannot be seen with the naked eye. Govender et al. (2015: 32) adds that if a vehicle is stolen, the departments may be unable to deliver its products. Customers who are waiting for their goods to be delivered may become irritated and seek alternative suppliers. This loss is not visible and is sometimes referred to as an indirect loss (Nyanchama, 2005: 31). The assets listed above are vulnerable to both violent and nonviolent crime. These crime risks pose a serious threat to the departments' profitability. Departments that are unable to manage their crime risks are frequently forced to liquidate and close. It is only necessary to read the financial sections of the local newspapers to become aware of this (Govender et al., 2015: 32).

According to Siboni (2011: 96), the STA approach makes it possible to evaluate several different aspects, such as the definition of defense-critical assets, management of communication, service continuity, technological management, reliance on external components, management of unforeseen incidents and accidents, the ability to assess the situation, and the identification and management of weak points. The review provides the decision makers with the information they need to establish a plan of action to increase the cyber resilience of the departments. Once this approach has been used to identify the departments that will be reviewed, the procedure is highly planned and well-ordered beyond that point. However, there is no foolproof way to determine which departments belong to which departments.

In order for the departments of a country to protect the critical assets of the country, every component of the infrastructure ought to be involved in the definition and implementation of a risk management programme (John & White, 2014: 16). This programme should include vulnerability analysis, risk assessment, and hazard mitigation procedures. The authors use the term "risk" to refer to a mix of what may happen, the possibility of that happening, and the negative consequences if it did happen. In addition, a "threat" is any kind of harmful action taken against an existing infrastructure (John & White, 2014: 16). A system is said to have "vulnerabilities" when it is susceptible to failures, disasters, or assaults (Nyanchama, 2005: 36).

The term "critical infrastructure" is used to refer to the significance of certain infrastructures (Onwubiko & Lenaghan, 2007: 11). Critical infrastructure is defined as the systems, facilities, assets, and networks providing critical national and economic security services for health, safety, and prosperity. The term "critical infrastructure" was coined by Onwubiko and Lenaghan (2007: 11), who define critical infrastructure as "large-scale socio-technical systems that offer services to society that are vital in the correct functioning of its institutions”. In its most basic sense, the term "critical" refers to important services that have the potential to undermine both the social and economic fabric of a nation in the event that they are interrupted (Thoka, 2021: 28).

The objective of the Critical Infrastructure (CI) Protection programme is to strengthen the physical and cyber security of essential governmental resources, while simultaneously limiting the effects of catastrophic events such as natural disasters, accidents in the workplace, and terrorist attacks (South Africa. 1980). In the international arena, the Canadian National Strategy and Action Plan for Critical Infrastructure (CNS&AP) was published in 2009 as a framework for the government's private sector's critical infrastructure owners and operators to collaborate on the security and resilience of critical assets (Public Safety Canada, 2019). According to Jagatic et al. (2007: 94), the spectacular breakthroughs in digital electronics are making it possible for both scientific advancements and dysfunctional results. This is because of the dual-use potential of these technologies. On the one hand, developments in digital electronics have the potential to raise overall quality of life, usher in new scientific discoveries, and promote overall productivity. Additionally, such developments and discoveries in digital electronics could be weaponized and utilised for targeting individuals, nations, and infrastructure.

Bayne and Friesen (2017: 5) highlight that "all hazards" idea would be utilised in the process of scenario development. It is possible to extrapolate the identification of threats and hazards, for instance, from one port of entry or key asset to additional ports of entry and risk settings. The threat scenarios would necessitate concentration on objectives and regions, and would include sufficient information to characterise the source, stakeholder, context, impact categories, time and space dependencies on essential infrastructure, as well as other critical decisions about information needs. The process of developing scenarios could be simplified by reducing the number of possible outcomes and preventing identical outcomes from occurring in different places.

Critical assets are those that are required to serve the social and commercial needs of both the local and national economies (Azad, 2008: 4). Critical assets can be found at both the national and local levels. If these assets are lost, it will have a significant impact; yet the likelihood of their loss is not necessarily very high. These assets should be identified separately and evaluated in greater depth as part of the planning process for asset management. By identifying vital assets, the authorities are able to target and improve their investigative processes, maintenance plans, and funding plans more precisely. One example of such an asset is a structure that is both unique and significant, such as a crossing of an estuary. Access to assets controlled by third parties, such as substations, which are only accessible via a single-track road, yet access to these assets is essential, may also be taken into consideration (PIARC; 2016).

After the STA team of the department has identified the vital assets, a decision should be made as to which assets are the most susceptible to attacks from violators and how security measures should be put into place and monitored (Singh, 2019: 8). Insider threats should be identified for each key asset, including those posed by privileged workers, service suppliers, and other stakeholders (Murphy & Randall, 2016: 27). The essential business operations of the departments, the staff and the clients, information, information technology assets, physical infrastructure, services, and intangible assets are all included in the definition of critical assets. It is important for the departments that have been designated as vital assets to work together in order to locate the employees who pose a high risk and make extensive use of these assets (Murphy & Randall, 2016: 27).

2.7 THE SCOPE OF SECURITY THREAT ASSESSMENT (STA) FRAMEWORK.

An essential component of any effective information security programme is the identification and analysis of potential vulnerabilities. Understanding risk in its most basic form is the first step in achieving security (Masse et al., 2007: 2). Nearly every information security strategy concentrates its efforts on locating and neutralizing dangers posed to government agencies and institutions. According to the Information Security, Threat Assessment is not a method that can be performed independently (Adetiba, 2017: 200). It is the initial step in the process that is collectively referred to as Risk Management. Information security is the primary emphasis of an Information Security Threat Assessment. However, risk management is a more comprehensive business approach that incorporates a wide variety of different types of risk assessments in addition to other components “such as analysis, mitigation, and so on” (Nkwana & Govender, 2017: 6).

Within government agencies, the SRA should follow a methodology that is easily understood (Nkwana & Govender, 2017: 6). The template has to be modified in such a way as to perfectly cater to the requirements of the various government agencies. An Information Security Threat Assessment Model (ISTAM) places emphasis on the following aspects: the scope and kinds of threats, assessment, risk level, vulnerabilities, likelihood, control degree of effectiveness, suggestions, analysis, impact, and final report (Andales, 2022: 11). The technique was developed to assist government departments and settings in effectively reducing the risks to their information security. Within the context of this model, assets have to be acknowledged as a component of the information security programme (Andales, 2022: 11).

According to Kuzminykh, Ghita, Sokolov and Bakhshi (2021: 605), assets and their values should be used in security threat assessment frameworks in order to assist evaluate the cost-benefit ratio between the value of the assets and the cost of prospective protection and controls.

According to Gritzalis et al. (2018: 5) and Kuzminykh and Carlsson (2018: 53), the implementation of security measures have to be predicated on an analysis of the dangers associated with the processing of information, establishing and maintaining a business continuity plan (BCP), detecting and investigating security breaches as they occur, training employees on security systems and procedures, taking steps to control physical security, implementing controls on access to information, adopting an information security policy; as well as taking steps to control physical security .

Isnaini and Solikhatin (2020: 77) identified physical information security evaluation as the suitable form of assessment for security information. Owing to its sole focus on physical and environmental controls, this form of evaluation could then be employed by government departments. Furthermore, this sort of evaluation may be completed fast and has the potential to uncover some high-risk items.

Employee assessments are required to be carried out on every single government worker who has access to confidential information. According to Patrick et al. (2016: 70), the Material Security Officer is obligated to take conducive steps to ascertain the dependability of every employee of the department with access to classified material in order to do their duties. This is an acknowledgment that personnel in the departments will inevitably have access to sensitive material. Disclosure of this kind should be limited to those workers who are directly affected by it, according to the concept of "need to know," because releasing it to anybody else would be a violation of that principle. Patrick et al. (2016: 71) underline that dependability of personnel should be considered during risk assessment, and that when sensitive material is involved, government agencies should pick individuals who are honest.

Sutherland (2017: 83) highlighted the need of security risk assessment as a crucial instrument for security, noting that implementing security solutions that rely on technology may be rather pricey. In order to secure information from unauthorised access, unintentional loss, or destruction, government departments should ensure that adequate security control mechanisms are institutionalised. These mechanisms should be tailored to the specifics of the data that needs to be safeguarded. Threats to a nation's cyber security constitute some of the most critical problems that many governments, including South Africa's, are currently facing (Patrick et al., 2016: 71).

2.8 ROLE OF DIRECTORATES IN GOVERNMENT DEPARTMENTS IN SUPPORTING SECURITY PROGRAMMES

Government departments in South Africa have each developed their own internal security procedures (Nathan, 2009b: 100). These members of the security personnel are also registered with the PSIRA. Civilian powers were granted to them in accordance with Act 51 of the Criminal Procedure Act in 1977. There are some in-house security professionals that are empowered to carry out their duties by national legislation that is connected to the individual government agency that they work for (South Africa, 1977). These professionals are engaged by specific government departments. They deal with information regarding events, risks, and vulnerabilities related to security on the proviso of the business case presented by the government department. The SAPS receives information on criminal acts so that they can investigate them. The information about the threat is received by the SAPS.

To limit risks, government departments address vulnerabilities by using security risk control procedures. Incidents involving policy violations are investigated by human resources internal investigators (Gumedze, 2008: 109). Meanwhile, security information is mostly gathered through security assessments (Gumedze, 2008: 109). Third parties also provide voluntary information. For instance, the public is provided with toll-free phone lines in order to collect 'hot-line' information. In some cases, covert operations are carried out in collaboration with the SAPS, which manually records the information into specified registers (occurrence book, case registers).

Security personnel in government agencies are primarily concerned with collecting data relevant to instances of policy violations, crimes, and other potential weaknesses (Mahlatsi, 2019: 06). They are better able to grasp the threats that the department faces because of the collection of information of this nature pertaining to security. The authorities are informed of all issues of criminality, and workplace investigators look into any policy violations that may have occurred. A significant amount of the information is lacking because most of the time, information is obtained belatedly or after the due date (Mahlatsi, 2019: 06).

In many instances, management analyses the acquired data and makes a choice on security risk control methods (Mahlatsi, 2019: 06). Accordingly, analysts are seldom used by departments to review, compile, and analyse data. In certain cases, regular clerks are utilised as analysts to determine crime trends and patterns. They collect and analyse data using computer software. The programme generates criminal pattern analysis products. Vulnerabilities are prioritised based on the threat they pose. Management considers the potential and repercussions of the danger in their meetings (Mahlatsi, 2019: 06). Under typical conditions, no formal study of risks and vulnerabilities is performed.

Security managers make security-related choices, depending on the information presented to them by other directorate in the departments (Nathan, 2009a: 27). Directorate Finance manages the day-to-day finances of the departments in accordance with the Public Finance Management Act (PFMA) and provides information to assist managers in making key strategic decisions (Moagi, 2009: 17). Their expertise can aid the Security Managers with information that has any irregularity or that contravene the PFMA and other prescripts on the part of the employees or third parties' involvement that warrants possible disciplinary, civil, or criminal action. On the other hand, the Human Resources Directorate is central to every department for employing personnel, terminating, payroll, and managing the database of the departments' employees (Nkwana & Govender, 2017: 14). The directorate should contribute to security programmes and aid in maintaining a secured environment. The information that is generated by this office is regarded as sensitive in nature, and includes the banking details of personnel, and their personal information. This renders the Human Resources Directorate a target for aggressors.

Furthermore, another directorate that has drawn widespread attention for wrong reasons is the Supply Chain Management (Palmer, 2016: 17). The high level of corruption involving supply chain employees and manipulating of tender process in government departments has been a concern for years, and that has compromised the integrity of security (Palmer, 2016: 17). The information about employees that involved in corruption and theft is not provided to internal security directorate for investigation. For years, the SSA has prioritised the SCM with the vetting processes. Hlengwa (2019) concurs that for some time now, SCOPA has demanded the vetting of senior government officials and executives of State-Owned Entities involved in procurement spending in SCM totalling hundreds of billions per year.

In the balance of probabilities, the information that can be gathered from all directorates in the departments, can aid security managers to ensure that the money spent on improving security measures is appropriate to what the departments seek to protect. Security control measures are performed in accordance with cost, provided the scenario justifies such costs (Palmer, 2016: 17). There was no evidence that a likelihood, effect, or cost-benefit analysis had been conducted in this respect. In many cases, there was a severe scarcity of workers, computers, and the necessary software to collect and analyse data. If further information is necessary, risk managers, security personnel, or investigators are utilised to gather it. All these should be conducted within the legal framework.

2.9 LEGAL FRAMEWORK TO DEAL WITH SECURITY THREATS

The SSA is primarily responsible for protecting South African government departments from both internal and foreign attacks (Africa, 2009: 62). The SSA's legal mandate provides certain obligations to the departments in terms of its intelligence and counterintelligence duty to preserve the country's national interests from both internal and foreign security threats (Africa, 2009: 62).

The risk of potential security breaches, as well as their severity, would rise dramatically in the event of South Africa's vital national institutions becoming inadequately protected (Cilliers, 2021: 1). In Section 1 of the National Strategic Intelligence Act, No. 39 of 1994, "domestic intelligence" is described as intelligence accruing from any internal factor, activity, or development that is deleterious to the national security and stability of the Republic of South Africa and its inviolable constitutional order, including the well-being and safety of its citizens (South Africa, 1994).

2.10 CURRENT LAYERS OF SECURITY MEASURES

In order to mitigate security threats, the government departments employ various security measures (Nathan, 2009a: 27). These are discussed in the following sections.

2.10.1 The South African Police Service

The SAPS is legally mandated to provide security advisory services and functions in relation to the layered security system and structure (SAPS, 2011). Figure 2.2 overleaf indicates the location of the Component: Government Security Regulators (GSR) within the SAPS national structure.

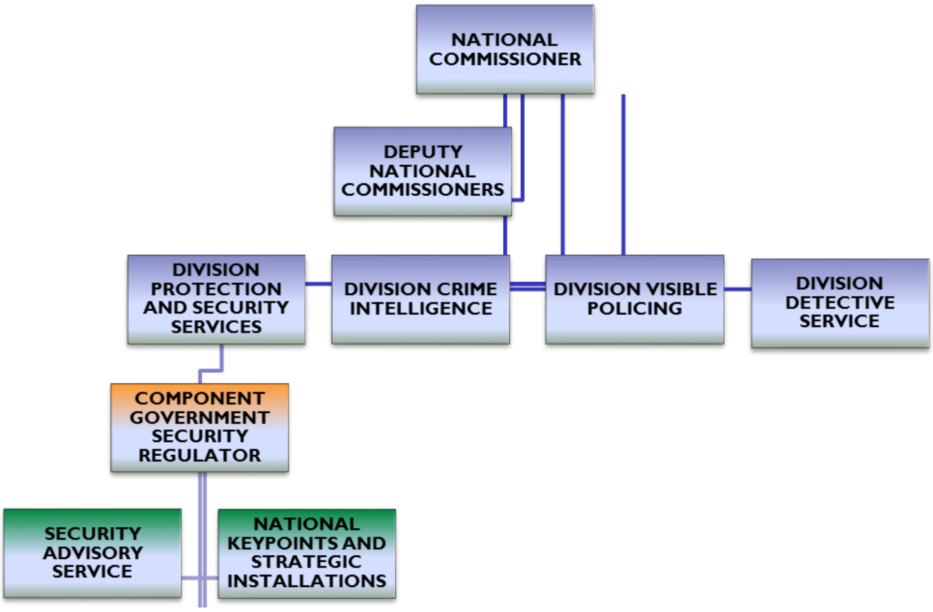

NATIONAL COMMISSIONER
DEPUTY NATIONAL COMMISSIONERS
DIVISION PROTECTION AND SECURITY SERVICES
DIVISION CRIME INTELLIGENCE
DIVISION VISIBLE POLICING
DIVISION DETECTIVE SERVICE
COMPONENT GOVERNMENT SECURITY REGULATOR
SECURITY ADVISORY SERVICE
NATIONAL KEYPOINTS AND STRATEGIC INSTALLATIONS

Figure 2.2: National structure of the SAPS
Source: SAPS, 2011.

The Cabinet decision of 2002 instructed that the GSR within the SAPS ought to regulate physical security in:

- Government departments;
- State-owned entities;
- National key points and strategic installations;
- Foreign missions in South Africa; and
- VIP residences.

The GSR functions include:

- Conducting physical security assessments;
- Identifying physical security breaches;
- Auditing existing physical security measures;
- Assist in monitoring the standard of physical security in government departments, parastatals (state-owned entities) and the SAPS;
- Assisting clients to conduct self-audits;
- Compilation of physical security assessment reports; and
- Conduct research regarding technology trends, capabilities and specifications of physical security related equipment.

The methodology of the GSR is premised on assessing the physical site on the government departments' buildings, conducting interviews with Security Managers and the management of the departments, as well as collecting data and conduct crime threat analysis (Palmer, 2016: 17; Philpott, 2013: 233).

Legislative frameworks are developed in order to exercise control over the country's practice of gathering information on criminal activity (Solove & Schwartz, 2011: 13). There are Lieutenant-Generals who serve as Provincial Commissioners, Major-Generals who serve as Cluster Commanders, Brigadiers and lower levels who operate at police stations, and a General who acts as the National Commissioner of the SAPS. The SAPS issues guidelines and guidance to its officers regarding the management of criminal intelligence and information. In terms of security information management, the SAPS checks information on criminal incidents, threats, and crime intelligence. They do not keep records of information on weaknesses in private security (Singh, 2019: 10).

The SAPS Crime Information Officers (CIOs) record all crime incident information that is reported by victims and complainants at the police station level on an automated Crime Administration System (CAS). The data is inspected by the supervisors one last time before the data capturers enter it into the automated systems (Singh, 2019: 10). This information flow starts at the local police station, then the automated system to the provincial office, and finally arrives at the national office. The official policy paper for MISS states that the information is protected via classification (Tilley & Laycock, 2018: 228). The information is accessible to everyone who has a valid reason to have access to it. Access to the information will be denied by the CAS if the person does not have the appropriate authorization to view it (Adetiba, 2017: 202).

At the level of police stations, the Business Intelligence System (BIS) is used by the Crime Information Analysis Centre (CIAC) to conduct an analysis of the crime data. Crime Information Officers (CIOs) are responsible for conducting field operations in order to acquire information regarding criminal activity through the use of interviews and visits to the scenes of crimes (Adetiba, 2017: 202). This additional knowledge on crime is typically used to address questions regarding the "what," "why," "where," "who," and "how" of criminal activity.

The new information is then used to enhance available information on the BIS in order to generate crime information products that may be used in police stations (Alshboul, 2010: 24). These products are intended to be actionable, and include case docket analysis, criminal statistical analysis, linkage analysis, crime pattern analysis, regional crime analysis and profiling; all of which are produced by the Crime Information Analysis Centres (CIAC) (National Crime Registrar, 2020: 4). At the level of the police station, the preparation of a document called a Crime Threat Assessment (CTA) is facilitated by the integration of all of the information that is contained inside these actionable crime information products.

At the cluster level, the CTA for this police station is connected with the CTAs for the other police stations in the cluster (National Crime Registrar, 2020: 4). Consequently, a Cluster CTA is produced. The data collected from the cluster stations is put through a process called linkage analysis. The result of the linking analysis is provided to Crime Intelligence Commanders at the Cluster level (National Crime Registrar, 2020: 4). The data is improved so that it may be used to offer intelligence on criminal activity. Criminal intelligence is deployed so that intelligence-led police work can be performed in the cluster in a manner that is effective, efficient, proactive, and reactive (National Crime Registrar, 2020: 4).

At the provincial level, the information gathered from the clusters is merged into a CTA document to be used for intelligence-led operations (National Crime Registrar, 2020: 7). This intelligence is reinforced by security service providers hailing from both the public and private sectors of the economy. The provincial office keeps a well-organised "War Room" that is used to collect information from these and other participants in the fight against crime. Crime-related information is not shared with other parties unless specifically allowed to do so by the provincial commissioner (National Crime Registrar, 2020: 7).

At the national level, the information provided by the Provincial CTA is analysed in order to combat organised crime through the use of novel tactics such as undercover and overt operations, physical and electronic surveillance measures, forensics, interviews, research, and audits (Knoesen, 2012: 33). Meetings of the Crime Combating Forum (CCF) are held every day at the station, provincially, and nationally with all stakeholders, including private security and other government departments. These meetings are intended to monitor and evaluate the application of information and intelligence through crime statistics, arrests, exhibit recoveries, and other similar means (Mabasa & Olutola, 2021: 5). All the information regarding potential dangers that was gathered from different external stakeholders, such as government departments and private security, was included into the CTA at various levels (National Crime Registrar, 2020: 7). The classification of information and how it should be handled are both governed by the guideline known as the Minimum Information Security Standards (MISS).

2.10.2 Minimum Information Security Standards (MISS)

The South African Government approved the "MISS" document as national information security policy on December 4, 1998. This document has to be followed by all government departments (Nkwana & Govender, 2017: 5). The goal of establishing this policy was to protect the country's national interests by measures of counter-intelligence. The "MISS" was created as an official government policy document on information security that all departments in the Republic of South Africa that handle sensitive or classified information should adhere to (South Africa, 1998).

Lee (2014: 44) asserts that government departments should develop similar security documents such as the “MISS”, as a policy guideline. The publication thereof should be provided to departments to stipulate how the policy will be enrolled, and what procedures would be followed (Sutherland, 2017: 90). The handling and management of information that is regards as classified is established by the MISS document (1998), which provide an obligation to all government departments. The "MISS" Cabinet document (1998), state that security measures should be implemented in all government department due to sensitivity of data that is in their possession. Such information will be graded in an appropriate classification and protected according to the degree of sensitivity.

As soon as the sensitive information that is under the jurisdiction of the departments is supplied with a special protection, such information will be regarded as classified information (Sutherland, 2017: 92). For instance, the lowest classification of information is “restricted", and refers to any information whose access is not authorised to any persons. This sort of information would be helpful for any kind of investigation in general. Meanwhile, information that is considered most sensitive is marked "Top Secret”, and is only accessible to employees and government departments with the necessary authority and approval on a “need to know” basis (Sutherland, 2017: 92). If disclosed to unauthorised individuals, this type of information would jeopardise the goals and operations of the particular department. In other words, this type of information has the potential to cause significant harm to government departments (Sutherland, 2017: 92). Control over the content of top-secret documents is maintained through a "Declaration of Secrecy" signature granting access to only government employees who can provide access to such information. According to the cabinet document "MISS" (1998), a Declaration of Secrecy, is an undertaking by a person who has, have had, or will have access to classified information that such information will be treated as secret (South Africa, 1998).

When deciding on the classification of information, government agencies should take accounting procedures into consideration. Accounting practices entail a set of policies, processes and checks that are utilised by an accounting department in order to produce and maintain accurate records of departmental activities (Beresford, 2015: 231). Ideally, the practice of accounting should be extremely consistent since a huge number of company transactions need to be handled exactly the same manner in order to create consistently credible financial statements. This is why it is ideal for the accounting practice to be extremely consistent. When conducting an audit of a firm's financial accounts, auditors rely on accounting practices that are uniform throughout the organisation (Bragg, 2014: 1).

In the event that accounting procedures are not taken into consideration during the information categorisation process, the deficiency may result in major vulnerabilities in the information security systems. Accounting procedures should be given great consideration by the government agencies because they constitute significant security controls (Surju, 2018: 17). As a consequence of this, careful thought ought to be given to the safeguarding of private financial information. Journals and ledgers are not the places where this type of information, along with purchases made with petty cash and things from supplies, should be freely documented (Nathan, 2009: 91). There should be accounting processes in place to manage sensitive projects in order to decrease the risk of the department budgets and their expenditures. These practices should guarantee that the sensitive information is not accessible to staff who are responsible with handling money.

Access to classified information should be restricted, according to the cabinet document "MISS" (1998). Access to classified material is restricted to only those individuals who are in possession of the necessary security clearance or who have been given an exception by the head of the departments, with the need-to-know principle being strictly adhered to at all times. In order for an employee to maintain their status as having a valid security clearance, they are required to go through the security vetting procedure (Sutherland, 2017: 92). According to the findings of the literature analysis that was carried out in the various government departments, this procedure is not carried out in line with the papers referred to as "MISS." The process of screening, verifying qualifications, doing background checks, and conducting thorough vetting investigations is part of the severe protocols that have to be followed while conducting employee vetting. The candidate should fill out a comprehensive personal history statement as part of the application process, which should serve as the beginning of the screening process for potential employees (Nathan, 2009: 91). In order to avoid recruiting unethical individuals who may leak secret information that may obstruct or inconvenience the operations of government departments, this should be done prior to an application being appointed in such agencies (South Africa, 1998).

Signing a Declaration of Secrecy either before, or while one is in the process of being appointed is another method according to the "MISS" cabinet document (1998) for the purpose of protecting sensitive or secret information (Surju, 2018: 17). The purpose of these announcements is to make a psychological impact on employees, reiterating the significance of maintaining the confidentiality of information that has been entrusted to them. It is possible to make the case that this procedure is not adhered to in its whole or is not followed each and every time by government entities. If an employee is found to have violated these declarations, they might be used as evidence in a judicial proceeding. These declarations are legal papers (South Africa, 1998).

The "MISS” cabinet document (1998) stipulates that any information that is labelled as secret or top secret should be kept in a secure location, such as a safe or a metal cabinet that is both of sufficient strength and is fitted with a locking mechanism (Lohrmann, 2021). This requirement applies to any information that is classified as secret or top secret. It is recommended that classified documents be stored in accordance with the following recommendations when they are not being used:

- restricted documents should be stored in the regular filing cabinet;
- confidential documents should be stored in the reinforced filing cabinet;
- secret documents have to be stored either in a strongroom or in a reinforced filing cabinet; and
- top secret documents" should be stored either in a strongroom, safe, or walk-in safe.

Lee (2014: 44) acknowledges that it is imperative to adhere to all of the required protocols in order to maintain the confidentiality of sensitive information. One example of this would be a standard that mandates the safety of all data processing facilities. In the absence of adequate storage facilities, sensitive government information will be put in jeopardy and will, sooner or later, become accessible to unauthorised parties (Sutherland, 2017: 92).

2.10.3 Information Security Programme

An information security programme refers to a comprehensive collection of technological, operational, administrative, and managerial procedures meant to secure the confidentiality, availability, and integrity of information in respect of business requirements and risk assessments (SAPS, 2011: 112).

The execution of the ISP places a large amount of responsibility on the shoulders of the many government departments. This might be accomplished by incorporating information security into the planning and operations of the departments as well as making it a component of the governance of the departments. According to Brotby (2008: 12), the plan has to be put into action by way of an all-encompassing ISP that includes thoughtfully formulated legislation and standards. The components of an information security programme include education and training concerning information security, risk assessments and impact analysis, information classification, as well as developing and testing plans for continuing business operations in the event of a disaster or service interruption. These security aspects ought to be incorporated into the overall ISP.

The administration of the information security programme within the department is tasked with ensuring that adequate resources are allotted in order to maintain the programme as a whole updated (Lohrmann, 2021: 23). In order for government agencies to successfully control information security, they need to design a sustainable framework that will drive the development and administration of an all-encompassing information security programme. This framework should also be kept updated (Lohrmann, 2021: 23). This framework will serve as the basis for the establishment of a complete Information Security Programme that is both cost-effective and accomplishes the goals set forth by various government agencies. This programme will be built on top of this framework. The primary goal of a security programme should be focused on ensuring the protection of government agencies' information assets to an extent that is proportionate to either the value of the assets or the likelihood that they will be compromised (Williams, 2017: 11). This should be accomplished by providing government agencies with the assurance that their information assets are protected.

This judgment was accepted by Solove and Schwartz (2011: 69), who went on to suggest that government departments should engage Information Security Managers to be responsible for implementation of security programmes in order to protect sensitive information. In addition, those in charge of information security should ensure that employees receive the appropriate training on how confidential information should be stored in order to achieve the highest possible level of protection. They need to ensure that the "MISS" implementation is carried out throughout all government departments, and then evaluate how effective it is.

A suitable information security programme should be intended to safeguard information against unauthorised access, alteration, disclosure, and destruction, in addition to accidental loss. This protection should also include the ability to recover lost information. Gutwirth, Leenes, De Hert and Poullet (2012: 220) all concur that government agencies ought to use audit trails in order to limit the accessing of sensitive information. Audit trails will make it possible to save records so that they can be used in investigations at a later time. In addition, government agencies should implement technology that enhances confidentiality and defends against invasions (Gutwirth et al., 2012: 221). Examples of such technologies are patching and encryption devices.

Alhassan and Adjei-Quaye (2017: 105) recommend the below-cited security measures in respect of protecting security information being accessed, altered, or disclosed in an unauthorised manner:

- To ensure that the departments lock files containing critical information in steel cabinets
- To ensure that the departments keep the files with classified information in a secured location which can only accessed by authorised officials
- To ensure that the departments protect the electronic data with unpredictable passwords
- To ensure that the departments restrict the premises containing personal information with cards method or passwords
- To ensure that the installation of computer monitors (including laptops) in visitors' areas (such as waiting rooms and showrooms), is accompanied by measures to prevent personal information from being accidentally disclosed to people who are not employees
- Developing an Information Management Policy that is distributed to all employees who handle personal information; and
- Ensuring that all personnel are trained to handle confidential information, and they conversant with the security measures.

Isnaini, Solikhatin and Bennett (2020: 80) emphasised on the relevance of the below-mentioned principles in relation to information security:

- The information that is generated for the use of officials should not be compromised or given to unauthorised people.

- Such information should be handled or accessed only by authorised individuals,
- The amount of information that is gathered and kept should be kept to an absolute minimum if one wants to accomplish a particular goal
- The security mechanism that a system should achieve should be communicated to and understood by the personnel and management, and it should encompass protections against the intentional abuse or exploitation of information; and finally
- A system of monitoring should be put into place to assist in detecting any violations of the security system.

Information security controls are categorised into three: operational, and technological controls (Kuzminykh et al. 2021: 605). Examples of technical controls include firewalls, as well as relevant software for virus protection, intrusion detection, and encryption. Protecting the organisation's information technology and the confidentiality of the data stored within these systems is the primary focus of these measures (Nkwana & Govender, 2017: 10).

Examples of operational controls include backup systems, restrictions on physical access, and environmental hazards (Kuzminykh et al. 2021: 605). Examples of operational controls include enforcement mechanisms for addressing deficiencies and various threats. Meanwhile, the use of policies, personnel training and BCP are examples of management controls that concentrate on non-technical aspects of information security. Management controls also include BCP (Patrick et al., 2016: 74). Concerns about information security cannot be resolved by technology alone. This is because information security is a social and organisational issue in addition to a technological one. Consequently, information security directors have priorities and resources that are assigned to support the entire objective of the organisation (Tilley & Laycock, 2018: 230).

Directors of information security should be alert to the types of sensitive information that need to be safeguarded, as well as the appropriate level of protection and the processes for securing such information (Patrick et al., 2016: 74). A security committee needs to be constituted, and the president of the institution should see to it that this happens so that proper consultation can take place with the heads of different business divisions.

2.10.4 Security Committee to Manage Security Threat Assessment

Most government departments have the security committees as part of compliance, but they do not function, neither do they take part in implementation of the STA (Watts, 2017: 12). A qualified security manager is at the helm of the SSA, and assisted by the security committee as required by the SSA (Watts, 2017: 12). The security committee comprises of the head of all sections or directorates in the departments. The inclusion of the section heads is to provide expertise and knowledge of their business units. When the STA Team has identified the critical assets and what need to be protected in every business unit, the process becomes clear, and the implementation become successful. Smith (2014: 17) agrees that the departments should form a threat assessment team comprise of specialists in every business unit. A threat assessment team includes members from various directorate within the departments, such as human resources, physical and information security, corporate management, or the legal section, as well as a stakeholder and a police officer from a local police station. Due to the risks and for support, a senior management or the accounting officers should also be involved.

David and Brydon-Miller (2014: 31) indicate that a threat assessment team is a comprehensive group that is not only capable of recognizing the vulnerabilities in the architecture of the departments but also delivers excellent context regarding the links between those weaknesses and other sorts of resistance diversity. A viable threat assessment approach involves a thorough grasp of the business landscape, the capacity to recognise weaknesses, knowledge of present threats, and the creativity to forecast new threats. The formation of such a team calls for painstaking planning and a strategy that is methodical in nature.

Blanchard et al. (2010) emphasise that the first consideration in building a threat assessment team involves the specification of each member’s duties. For instance, the breadth of the obligations within the purview of the group determines whether or not the team will need to undertake vulnerability assessments; or whether or not other sections of the departments that may currently supervise this activity may be leveraged instead. There should also be a determination of the extent of the reports and suggestions that should be received from the team (David & Brydon-Miller, 2014: 31). The team should conduct investigations, gather information, and also monitor the department’s progress insofar as implementing recommendations, or whether this task should be delegated to another group that is already in existence (Smith 2019: 188).

When emotions are at a peak, it could be difficult to distinguish between gossip and fact. The investigation team has to identify the persons involved, the role of witnesses, as well as any background information of relevance that has been directly obtained from the source (Smith 2019: 188). The STA and management team should aim to enhance the departments' protection proactively (Smith, 2019: 188).

It is very important that the core business of the department is understood, that the critical assets are identified, that the scope of STA is clearly defined, and that the role and responsibilities of the team are understood (Sutherland, 2017: 101).. The researcher is of the opinion that when all the directorates are well represented by subject matter experts, the STA becomes easy to implement because they know which assets are critical, information is sensitive and which people are attached to those assets. After the team is put together, the researcher focused on inclusion of mental practitioners in the process of threat assessment (Sutherland, 2017: 101).

2.11 INCLUSION OF MENTAL CARE PRACTITIONERS

The use of STA has developed over the years and has received its cues from assessments of the potential for violent behaviour that are carried out by psychologists and other specialists in mental health (Cockerham, 2016: 17). Each day, in the public sector, the commercial sector, as well as in law enforcement organisations, there are specialists toiling away at the task of detecting and preventing these wanton deeds from ever happening in the first place. The professionals in charge of danger assessment and threat management are the ones responsible for these less reported, but no less serious interruptions (Singh, 2019: 8). The researcher contends that the practitioners in security and intelligence bodies do not work jointly with providers of mental health care and other security stakeholders who are already working collectively and systematically in assessing the risk of violence in the workplace accurately, and then take concomitant steps to mitigate such risk. According to Burgess (2018: 1), it is essential for professionals working in the fields of law enforcement, criminology, and mental health to understand how the STA can be utilised to create effective tools for the prevention of violence (Cockerham, 2016: 17).

Mbowe et al. (2014: 166) use a broad definition of STA as a set of operational and investigative techniques utilised by law enforcement professionals to assess, identify, and manage the risks attendant to targeted violence and its likely perpetrators. Such a definition is cognate from Fein, Vossekuil, and Holden's (1995) definition of STA, which is posited as the process of acquiring information in order to comprehend the danger posed by the targeted individual or group (Mbowe et al., 2014: 166-167). The American Psychological Association outlines an approach to threat assessment that includes a wide variety of activities. These activities are intended to identify and intervene with potentially violent individuals, as well as to avoid instrumental violence like a shooting at a workplace. Its purpose is to prevent violent situations and to "help potential offenders in overcoming the underlying origins of their anger, hopelessness, and depression.", or "despair" (NASP, 2014). This strategy focuses on determining the threat that is posed by a certain person carrying out a particular attack. This individual could be an employee who has threatened other employees, or recently involved in altercations at work.

The researcher is of the opinion that there is a significant disconnect between the security departments and the HR departments, and that HR is hiring people without properly vetting them. In many instances, a newly employed person rushes to sign up for a labour union to ensure that he/she has a voice in the workplace (Cockerham, 2016: 17). It is only the subsequent vetting process that will discover the particular employee’s past in the form of a history of violence, a personal grievance, a criminal record, substance abuse, or mental health issues. At that stage, it becomes difficult for the departments to terminate their employment without engaging the labour unions (Cockerham, 2016: 17).

Many perpetrators of security threats are known to have one or the other of the above-stated social behavioural factors that necessitated vetting (Cockerham, 2016: 17). These social and behavioural aspects can act as warning signs to help identify those who are at risk of engaging in instrumental violence. The researcher agrees that some of the employees' aggressive behaviour has mental health undertones and that these employees are either victims of abuse or they themselves are abusers (Cockerham, 2016: 17). These aspects are not evaluated as part of the STA because the security manager never invites the department's employee mental care practitioners to participate in the event.

In the United States, the National Terrorism Advisory Committee (2014), which focuses on schools, states that the approach to school-based threat assessment consists of the following steps:

- establishing a limit for law enforcement intervention and an investigative-driven threat assessment process, or refer individuals based on a variety of factors such as motive, communications, weapons access, stressors, emotional and developmental issues;
- assembling a multidisciplinary threat assessment team, and identify behaviours that necessitate intervention (for example, carrying a weapon or making threats);

- establishing and training on a central reporting system; and
- establishing a limit for law enforcement intervention (NTAC, 2018).

The researcher is of the view that the strategy can also be extended to the facilities of government agencies, and that the police station where the departments are headquartered should take part in danger assessments to provide an overall picture of the threat level posed by criminals in the area.

Individuals who are potentially dangerous can be located with the use of information and referrals (David & Brydon-Miller, 2014: 37). These individuals can also be evaluated for their likelihood to carry out an attack. As part of this method to threat assessment, a range of interventions are directed toward the individuals who are at risk of committing violent acts. In the event that an attack is about to take place, law enforcement officials may take more urgent measures to get control of the individual (David & Brydon-Miller, 2014: 37). Assessments of the potential for violence are largely clinical and legal in character. They consist of predicting the possibility that an individual will engage in violent behaviour in the future as well as locating risk factors and intervention measures. This approach is distinct from the threat assessment that was discussed earlier with regard to instrumental violence.

The propensity for violence in general, rather than a specific attack against a specified target, is the focus of this method for determining the likelihood of an individual committing an act of violence (Nkuna, 2020: 22). This technique to risk assessment might not be something that the departments or their people carry out directly; rather, these assessments are typically carried out by doctors who have prior experience in the field. These violence threat risk assessments can be utilised in the decision-making process for the release of an individual from a penitentiary or psychiatric facility, as well as for civil commitment, criminal punishment, or categorisation after admission to a correctional or treatment facility (Nkuna, 2020: 22).

As part of this assignment, a clinical expert may administer a series of tests in order to assess the individual's propensity to commit an act of violence (Rees, 2016: 14). These evaluations of the potential for violent behaviour may incorporate both actuarially based findings and the clinician's own professional opinion. Assessments based on actuarial theory make use of predictive algorithms to analyse many risk variables in order to arrive at a conclusion on the likelihood of violent behaviour. The professional judgment of seasoned assessors can also be utilised in the interpretation of these actuarial-based model (Rees, 2016: 14).

According to Ali (2021: 2), mental illness was discovered in both female and male stalkers, and stalkers with mental diseases were more likely to engage in violent crimes. It was also found out that females will stalk acquaintances and participate in a variety of different stalking behaviours. The afore-cited authors further describe stalking as invasive conduct that is carried out on two or more times and that causes concern or terror in the targeted individual. According to the statistics, the majority of those who are stalked are male, whereas most of their victims are female. Although it has a substantial impact on victims, stalking committed by females has gotten less attention than stalking committed by males. The low rates of female-perpetrated stalking research, reporting, and understanding is attributed to the rigid societal beliefs that female-perpetrated crime is not deserving of being taken seriously or is somehow less intrusive (Ali, 2021: 4). The latter authors further confirm that victims usually encounter a lack of support, which is one of the primary reasons for unreported incidents of female-perpetrated violence.

The researcher encourages the cross-discipline collaboration in the practice of threat assessment and threat management, as well as sharing of expertise between disciplines. The researcher upholds the view that the involvement of mental care practitioners will make a huge impact in preventing the workplace violence and sexual offences cases which are difficult to prove.

2.12 SUMMARY

The chapter reviewed current literature on security threats assessment by exploring the current internal and external threats that South Africa is facing presently. Firstly, the researcher contextualised and operationalised the term, ‘threat assessment’ for the purpose of this study. The researcher further explored the different types of threats, including cyber security threats, external threats that are linked to illegal immigration, and the threats to the country’s critical infrastructure. The STAF was explored as ideal for the development of effective strategies of mitigating security threats in government departments. In support of the framework, the role of the government directorates was reviewed, as well as the various layers of security measures to mitigate security threats. The next chapter presents and discusses vulnerability assessment in relation to its associated contextual factors or variables.

CHAPTER 3
VULNERABILITY ASSESSMENT

3.1 INTRODUCTION

The STA is helpful in the identification of vulnerabilities in the existing security measures, and in the core business of the departments. Vulnerabilities are weakness and chasms that exist within the security controls and that need to be mitigated to ensure that a department executes its primary mandate effectively. In this chapter, the researcher discusses the complexity of identifying flaws in the security programmes and weakness in structural, procedural and elements of human factor that compromise the assets of the departments. Furthermore, this chapter discusses the direct importance of vulnerability assessment, composition of teams, the implementation steps, report outline and rating methods. The chapter also encapsulates vulnerability assessment as a vital aspect of the risk assessment model in the prevention of increasingly complex and sophisticated attacks from aggressors.

3.2 THE CONCEPT OF VULNERABILITY ASSESSMENT

The term "vulnerability assessment" refers to the systematic process of locating, defining, categorising and ranking the severity of breaches in network infrastructures, applications, and computer systems. In addition, vulnerability assessments equip departments with the knowledge, awareness, and risk context they require to comprehend the dangers posed by their surroundings and formulate appropriate responses accordingly. The identification of potential dangers and the associated risks is the purpose of any vulnerability assessment procedure. They often involve the use of automated testing tools, such as network security scanners, the results of which are then reported in a vulnerability assessment report (Rosencrance, 2022: 14).

Renfroe and Smith (2016: 20) mention that security risk threat assessment precedes the assessment of vulnerability. Such vulnerability evaluation is categorised into two distinct sections. Firstly, it involves an assessment of the potential loss that could arise from a successful attack at a particular place. In other words, the cost of a particular facility stopping to provide its services. This can be thought of as the amount of money that would be lost. Secondly, vulnerability assessment is based on the evaluation of a target’s vulnerability in the event of a planned assault. Vulnerability assessment is also construed as a categorisation of the strength levels that are already in place against any type of danger.

According to Renfroe and Smith (2016: 13), a significant amount of disruption would be incurred in the event of a large airport deciding to halt operations for any amount of time due to its location in a congested metropolitan region, where there are no other airports nearby. If one compares the attractiveness of different airport operations, one could find that a large city airport is a more desirable goal than a small county airport. Furthermore, risk assessment focuses on potential dangers, the consequences of losing a facility, and assessments of one's susceptibility. In this regard, the risk assessment requires an analysis of the preventative measures that are already in place as well as those that will be required in the future. Based on the findings of this investigation, it appears that the present countermeasures might be updated or made more effective with modification.

Meanwhile, a security vulnerability assessment relates to the process of identifying, characterising, and categorising security weaknesses and the possibility for criminal conduct in relation to a security system and/or programme. It conducts risk assessments, establishes the severity of the danger, and makes recommendations for solutions that have been proved effective in the industry. During the security vulnerability assessment, it is possible to determine high-priority weaknesses and their susceptibility to adversity and exploitation, as well as the consequences of such a breach on the security of departments. It is the duty of the departments to utilise the results of a security vulnerability assessment report in order to identify the asset protection measures necessary for decreasing or eliminating any risks posed to those assets (White, 2014: 167).

White (2014: 167) further asserts that vulnerability analysis will be a component of a larger security risk assessment in many situations. Both vulnerability and security risk assessment often precipitate the efficacy of proposed remedial measures. In addition, the final report needs to provide the reader with an idea of the anticipated effects after the recommendations have been actioned.

Garcia (2006: 02) suggests that it is essential to make a distinction between safety and security measures when considering vulnerability assessment. Safety measures relate to any actions taken with the intention of preventing or detecting an abnormal state that threatens the well-being of individuals, property, or business. This category of safety-related actions includes unplanned occurrences, such as accidents caused by human error or negligence, inattention, and poor training. On the other hand, security relates to precautions taken to protect people and property from the hostile actions of others. Civil unrest, sabotage, shoplifting, theft of essential goods or information, violence in the workplace, extortion, or other purposeful acts. Wallis (2022: 25) agrees with Garcia (2006: 02) that, it is inevitable for humans to make mistakes, and since defects are the result of software being authored by humans, it is inevitable that software will contain problems. There are many problems, and most are not harmful in any way. However, some problems tend to be vulnerabilities that can be exploited, which puts the system's usability and security at risk.

The next step involves conducting a vulnerability assessment, which is an evaluation of the vulnerabilities that exist in information technology systems at a particular point in time. The purpose of this investigation is to discover faults in the system before hackers are able to exploit them. According to White (2014: xiii), the practice of identifying risks and vulnerabilities has significantly improved over the years, and it is now more widely recognised than it has ever been as a standard approach. Therefore, professionals in the field of security need to have a better understanding of how to evaluate security threats and document their findings in the context of perpetual change. Researching the topic and acquiring experience in a range of settings is frequently the most effective way to educate oneself on how to carry out activities of this nature.

Allen (2016: 31) alludes that a security vulnerability analysis is the examination of the underlying factors of a security breach. Such analysis involves the physical, operational and technical controls to prevent, postpone, and minimise the impact of a vulnerability incident on the departments. The security vulnerability assessment provides higher management with proof that vulnerabilities exist and assists in the acquisition of funds for solutions. These enhancements could include a security programme implementation, the acquisition of new technology, the performance of modifications to lighting or other aspects of physical security, the provision of training, an increase in awareness, and so on. The assessment of vulnerability is an essential part of the risk assessment model, which includes an examination of numerous important location aspects.

According to Rosencrance (2022: 14), much could be gained from conducting vulnerability assessments. regardless of the size of the personnel or department that is susceptible to the attacks by computer criminals. This is true for both the departments and their personnel. However, huge department and any other departments that have regularly been invaded by aggressors can also benefit from vulnerability analysis. Therefore, vulnerability analysis focuses on identifying weak spots in a system. It is essential for companies to locate and fix any security holes in their IT systems and applications before they are exploited by hackers. As such, security issues can make it easier for hackers to access IT systems and apps. When combined with a management programme, a comprehensive vulnerability assessment could be of assistance to the departments in strengthening the level of protection afforded to their respective systems.

In cases of cybercrime, a passive vulnerability is a weakness or flaw whose exploiting effects are unobtrusive or invisible, but which can nonetheless contribute to overall cyber dangers (Mbanaso, 2021: 14). An active vulnerability is one in which the repercussions of its exploitation are clear, obtrusive, or conspicuous, with obvious contributing impacts to the totality of cyber threats. Active vulnerabilities have the potential to be exploited by hackers. Mbanaso (2021: 15) differentiates between two different forms of cyber vulnerability classification, namely: government function and organisational function. The government is responsible for a variety of tasks, including those of a legal, institutional, and technical nature. Examples of organisational functions include people, procedures, and technological advancements. According to Mbanaso (2021: 15), the legal, institutional, technical, people, and process functions are all examples of passive functions with consequences that are either unnoticeable or difficult to identify. Technology is an operational function that produces consequences that are intrusive, visible, or noticeable.

In recent times, there has been a precipitous rise in the number of different vulnerability situations that can occur in automobiles. A level of complexity that has never been seen before has been brought about due to the expanding interconnection on varying architectural layers (for example, electrical control units, diagnosis, configurations and their changes, software components, telematics, and communication both inside and outside the car). It is just a matter of time before whosoever is seeking to take advantage of the resulting loopholes and vulnerabilities can identify them and use them to their advantage. Connecting a device to any given location on a bus system that is frequently used can create conditions that, in time, will lead to the system's failure to work properly. This theory has previously been tested and proven, and it applies to bus systems such as CAN and Ethernet. Accordingly, device connection to any point on one of these bus systems could be performed externally at any time (De Gruyter, 165: 2021).

The security survey results are categorised and summarised in the vulnerability assessment portion of the security risk assessment report. Any potential attack vectors are also listed in this section. The weaknesses and shortcomings of the security programme should be sufficiently detailed in order to assist in selecting and implementing appropriate solutions (Vellani, 2020: 96). When analyzing a system's susceptibility to attack, it is important to consider not only the departments, but also the peculiarities of each individual. For instance, factors such as one's position, age, gender, race, nationality, and sexuality might all have an effect (Bickley, 2017: 29). Following the completion of a security assessment, the security managers will have complete control over the safety of the departments. Solutions will be presented that will assist in making the assets more resistant to criminal activity and in preventing criminal activity from ever occurring in the first place. All potential dangers and openings in the security of the departments will be unearthed and analysed (Mandell, 2013: 05).

Despite the indispensability of a technology-driven security programme, it could still be rendered an ineffective control against some vulnerabilities (Allen, 2016: 72). In that regard, technology is an important part of every security programme, which necessitates the institutionalization of a comprehensive regime of security measures in the form of an all-encompassing approach that integrates physical, technical, and operational safeguards in its day-to-day business activities. It is difficult to under-estimate the complexity of a security programme and attaining security cannot be accomplished by putting a single control in place. Rather, security should be achieved through a combination of controls. The concept that "one size fits all" will never be appropriate when it comes to the management of wide security vulnerabilities and the execution of a security programme since there is no such thing as "one size fits all." A corporation is exposed to a wide variety of different kinds of general threats, and security is simply one of them. Enterprise risk management, often known as ERM, is a process that involves assessing and ranking all of the potential threats to a business, with security being one of those threats.

Allen (2016: 72) propounds that a security assessment or security vulnerability analysis constitutes a sub-component of enterprise risk management, and that this sub-component includes a security assessment or security vulnerability analysis. For instance, the vulnerability of assets, people, companies, brands, and reputations might all be seen as security risks from the perspective of enterprise risk management (ERM). An organisation would be subjected to a security vulnerability assessment in order to determine, verify, and rank the vulnerabilities that are capable of resulting in a security breach in order to enable an evaluation of this risk. This assessment would be performed in order to determine the likelihood of a security breach’s occurrence. This incident could appear insignificant, such as product loss; or it could be something very serious, such as a shooting that took place at one of the facilities.

According to Allen (2016: 31), a security vulnerability analysis examines the underlying reasons of a security weakness or breach and implements physical, operational, and technical controls to prevent, postpone, and lessen the impact of an incident on the departments. The security vulnerability assessment provides higher management with proof that vulnerabilities exist and assists in the acquisition of funds for solutions. These enhancements could include the implementation of a security programme, the acquisition of new technology, the performance of modifications to lighting or other aspects of physical security, the provision of training, an increase in awareness, and so on. The assessment of vulnerability is an essential part of the model of risk assessment, which includes doing an examination of numerous important aspects pertaining to the location. The evaluation of man-made effects will centre on this aspect.

The most effective security approach is one that generates the highest possible level of awareness of potential threats with the least amount of effort and expense. In general, the first benefit is that there will be an awareness of the vulnerabilities that these systems and components are susceptible to. Secondly, if the enterprise leadership or the plant owner or operator does not take action to mitigate and repair the vulnerabilities and hazards that were discovered in the security assessment, then the assessment is useless. As a consequence, the risk assessment is a group effort, with members of the assessment team highlighting vulnerabilities, determining the level of risk (critical, high, medium, or low), and recommending ways to mitigate the risks in order of priority, starting with the risk that poses the greatest threat to the organisation and working their way down to the risk that poses the least threat (Heyden, 2020: 100). When departments are put in a position where they are exposed to a high level of risk and vulnerabilities, they are likely to experience many security breaches. This helps them to realise the criticality of carrying out a vulnerability assessment.

3.3 IMPORTANCE OF VULNERABILITY ASSESSMENTS

White (2014: 168) argues that a security vulnerability assessment serves as a form of standard for all the various protection measures. When executed properly, the purpose of the risk assessment is to compile a list of all discoveries and executing a plan for mitigating, avoiding, and reducing the impact of the risk discovered. Policies, operational systems, and processes are the most common elements of an effective vulnerability assessment. If the departments have a security policy that restricted access to a particular area and demanded that all visitors be always escorted, the security professionals could choose to test this requirement to determine whether individuals could enter the area without being escorted. This would allow them to determine whether individuals could enter the area without being escorted. As such, they would be able to decide whether the policy was genuinely required. A great number of departments have recently arrived at the conclusion that, regardless of the existence of rules, operational protocols, and security systems, there is still some degree of vulnerabilities that may be exploited by malicious actors.

According to Sahoo (2021: 23), vulnerability assessments ought to be mandatory for all departments, regardless of size, to guarantee the complete safety of their information technology infrastructure. These in-depth evaluations not only shield businesses from the dangers posed by malevolent cyberattacks, but they also contribute to the establishment of a credible stance in the eyes of customers and other stakeholders. According to Sahoo (2021: 23), the approach of vulnerability assessment utilised by the department is impacted by the department's one-of-a-kind environment, the one-of-a-kind threats it encounters, and the department's particular security requirements. The information that is obtained from a vulnerability assessment is invaluable, and this is true regardless of whether the department’s handling the vulnerability assessment do it with an internal security component or with the assistance of an expert external service provider. Because the primary objective of conducting the assessment is to lower the department's risk, the process has to be carried out on a consistent and timely basis. Additionally, it should consider any potential security threat before it manifests itself to guarantee that the departments' processes are carried out effectively.

According to Jaafor and Birregah (2017: 108), a precise vulnerability assessment of a social engineering system attacks is advocated, as a component of a policy to prevent social engineering. The modelling of threats from social engineering assaults has received little attention, leaving security personnel to rely on models designed for other objectives, such as network vulnerability assessment. This occurs in spite of social engineering’s severe repercussions. Monitoring a variety of different blogs, forums, and social networks would make it possible to reveal valuable information regarding the channels that are preferred by social engineers, most vulnerable users to social engineering trends and attacks, and the most common approaches that are utilised by social engineers.

The departments receive information about any holes in their environment's security that are discovered during a vulnerability assessment. In addition, it discusses evaluation of the risks that are connected to certain flaws. This method gives the departments a better awareness of their assets, security issues, and overall risk, which reduces the possibility that a cybercriminal will be able to break into their networks and surprise them (Rosencrance, 2022: 127). Wallis (2022) contends that there is a significant gap between presumption of a cyberattack vulnerability and precise knowledge of the vulnerability mode. This is due to the inability to thwart a cyberattack unless its precise level of vulnerability is known. The purpose of conducting a vulnerability assessment is to narrow this void. During a vulnerability assessment, some, or all the systems are investigated, and a thorough vulnerability report is generated as a result. After that, this report can be utilised to rectify the problems that were found to prevent any security breaches.

Additionally, a growing number of departments are technology-dependent for their primary mandate, yet cyber threats such as ransomware can instantly bring an end to the fundamental company operations. Both the importance of cyber security and the demand for solutions that assure its resilience have increased as a result of the common realization that it is better to prevent problems than to treat them. For instance, an increasing number of service providers increasingly demand frequent vulnerability assessments, and proof of security testing can be helpful to the operations of the departments (Wallis, 2022: 13). Security managers should keep in mind that different departments have different missions and visions, and they should consider using a variety of vulnerability assessments to verify that the solution they choose addresses the actual issue.

3.4 TYPES OF VULNERABILITY ASSESSMENTS

According to Rosencrance (2022: 127), vulnerability assessments are useful for locating a variety of different sorts of system or network problems. This indicates that the process of assessing the system would involve the utilisation of a wide variety of scanners, tools, and procedures to discover threats, vulnerabilities, and hazards. Following are some of the vulnerability assessment scan types that can be performed:

- Potential breaches in network security can be identified using network-based scanning. This form of scan is able to identify vulnerable systems on wired as well as wireless networks;
- Vulnerabilities in servers, workstations, and other network hosts can be identified and located with the use of host-based scans. A scan of this kind will often investigate services and ports that can also be discovered using network-based scanning. However, it does enable more prominence of the configuration settings and patch history of all systems that have been scanned, including legacy systems;
- Vulnerabilities in the wireless network infrastructure are often the primary focus of examination during wireless network scans performed on an organisation's Wi-Fi networks. In addition to locating risky points of access, validating that a company's network has been established securely can be accomplished using a wireless network scan; and
- Application scans for known software vulnerabilities as well as inappropriate network or web application setups on websites. Database scans help detect vulnerable areas inside a database so that malicious attacks like SQL injection assaults can be avoided.

Sahoo (2021: 24) observes the different types of vulnerability assessments to acquire better understanding of the tests performed and the scope covered as follows:

3.4.1. Wireless Assessment

When conducting wireless assessment, several architectural, environmental, and configuration variables with an immediate impact on the safety and functionality of the current wireless installation are evaluated. These variables include this entails analysing all of the wireless access points and mapping out their locations across the environment.

To further enhance the systems and procedures, this would also include doing an assessment of the physical installations, such as the orientation and mounting of access points. If the departments decide to hire a service provider to carry out the vulnerability assessment, the provider will identify the wireless networks and evaluate the wireless security controls. These controls include access management, encryption, and authentication. When evaluating the efficacy of wireless encryption techniques, as well as the setup of wireless access points and wireless cards, Sahoo (2021: 23) includes this information in their analysis. These types of testing involve first attempting to find known as well as unknown vulnerabilities, and then recommending ways to protect against those vulnerabilities.

3.4.2. Build Assessment

Build assessment is the practice of examining different versions of a piece of software or programme for defects in either its performance or its level of security. These vulnerabilities in the application's security could, at some point in the future, cause performance issues. In addition, malicious software and hackers routinely search for exploitable security holes and loopholes in order to break into a system. Because of this, a build vulnerability assessment can support a consistent examination of the layouts of the applications and systems, as well as the design of the security systems and the technology that is currently utilised in the setup. This helps to prevent or control the accumulation of vulnerabilities that are caused by faults in either the system's performance or its security.

3.4.3. Web Application Assessment

Sahoo (2021: 22) alludes that this kind of evaluation can find vulnerabilities in the system by using automated front-end scans, by carrying out either dynamic or static code analysis, or both. It is an essential approach for web-based and cloud-based application development. The executing code of an application is the primary focus of Web Application Scanners, whilst the webserver and its operating systems are analysed by Network Vulnerability Scanners.

In contrast with other vulnerability scans that utilise a database of identified vulnerabilities and misconfigurations, web application vulnerability scanners are specialized tools that search for well-known types of web flaws, such as cross-site scripting (XSS), SQL injection, command injection, and path traversal. Web application vulnerability scanners can be found online. Other vulnerability assessments make use of a database that contains information on known flaws and configuration errors. It is likely that they will identify vulnerabilities that have never been found before and that are specific to the application that is now being analysed. Those that do penetration testing frequently make use of this approach, which is also known as Dynamic Application Security Testing (DAST).

The source code of web applications is analysed while they are still in the development stage by use of a set of tools known as Static Application Security Testing (SAST). These are used in combination with SAST. As part of the procedure known as secure development lifecycles, this is carried out (SDLCs). Because of this, so-called interactive application security testing (IAST) tools—which are supplementary to static application security testing (SAST) and dynamic application security testing (DAST)—

are frequently used to incorporate Web Application vulnerability testing into DevOps and QA processes. The IAST facilitates the identification of vulnerabilities and dangerous configurations that may exist in applications prior to their launch or use in production. This is helpful since vulnerabilities and unsafe configurations may exist in applications.

3.4.4. Database Assessments

The Database Security Assessment is the procedure of locating flaws or vulnerabilities in database management systems like Oracle, Microsoft SQL, MySQL, Postgres, and others (Sahoo, 2021: 21). The sensitivity of a database to a predefined collection of attack and vulnerability scenarios are the first risk element that has to be evaluated.

Sahoo (2021: 22) adds that such vulnerability could be the result of an error of configuration, such as the absence of a database password policy; a misconfiguration of critical files, such as the configuration of the listener or audit trail; or a privilege management error, such as public access to a sensitive table. Alternatively, this vulnerability could be the result of a lack of a database password policy.

3.4.5. Host-based Assessment

Host-based vulnerability assessment is a process for providing detailed understanding of the possible internal and external risk exposure and business impact. It is an in-depth evaluation of networks and systems to identify security weaknesses that should be addressed.

The assessor then scans the system from the viewpoint of a user within the departments that may possibly access the network/system. As such, this assessment provides information on potential insider threats to networks and systems. The evaluation assists in identifying suspicious insider activities and detecting intruders who have already infiltrated the system. As a result, the host-based assessment augments an additional security layer in order to help prevent internal misuse or external intruders from compromising access to, and information security.

3.4.6. Secure Configuration Assessment

It is absolutely necessary to conduct a risk assessment on the systems and networks that are used by a department (Sahoo, 2021: 26). Accordingly, the Secure Configuration Assessment (SCA) is an examination procedure that helps in the discovery of vulnerabilities in the underlying infrastructure configuration. This covers the configurations of routers, switches, servers, mainframes; as well as the firewall and adequacy of the department's DLP security matrix.

The assessment helps in the identification of the likely vulnerabilities and configuration issues in applications and systems that a hacker could exploit to obtain access. Consequently, the assessment provides insight into the existing security posture, in addition to providing a comprehensive analysis of access restrictions, applications, and applications running on vital systems, as well as identifying missing security patches.

3.4.7 Mobile Application Assessment

Mobile application evaluation refers to the process of analysing mobile software to determine whether or not it is safe to use and unaffected by any potential dangers. An analysis of the mobile applications and the application programming interfaces (APIs) is carried out by the specialists so that they can determine the level of protection that these programmes offer against both known and unknown dangers. This helps in finding vulnerabilities and applications’ possible exposure to risk, such as password storage, session management, and ‘middle-man’ attacks.

Evaluating both dynamic and static mobile security testing methodologies is a part of the security assessment that is being carried out. It is an evaluation that involves a look at the protections against privacy breaches, as well as the application's behaviour and security measures. In its whole, the evaluation reduces risk exposure, boosts operational efficiency, implements actionable security measures, guarantees protection of applications from any likely dangers, and resolves statutory compliance requirements.

3.5 FORMULATE A VULNERABILITY ASSESSMENT TEAM

Vellati (2022: 83) illuminates that the team performing the vulnerability assessment concentrated on each individual’s element of the physical protection architecture in turn, beginning with the preventative measures. The most common types of measures of deterrence include lighting, signage, highly visible, uniformed security personnel, and other countermeasures such as natural barriers and fencing. These deterrence measures have the potential to intimidate potential attackers and tip the risk-reward balance in security’s favour. The detection procedures that are a part of the physical security system also need to be addressed. It is important to implement security detection systems not just within the building, but also around its perimeter to reduce the amount of time that passes between an incident being discovered and the security team taking action. These measures do not include only the installation of interior and exterior intrusion detection systems, but also the installation of each system's individual components, such as sensors, clear zones, and closed-circuit television systems. Vellati (2020: 83) states that during the security survey, the vulnerability assessment team should resolve the following issues:

- What is the major control process that has to be performed?
- What kind of checks are performed on the parcels before they are permitted inside the facility?
- Does the screening of individuals and parcels involve the use of X-ray equipment, magnetometers, or just eye inspection?
- What kinds of access control procedures do you have in place to make sure that only authorised employees may enter the building?
- Does the location have more than one point of entry?
- Are the exiting vehicles of sensitive regions subject to screening?
- Do the intrusion detection measures, such as sensors, around the perimeter of the building work as they should?
- Can the sensors' capacity to identify an entry be hindered by external conditions such as the topography and the weather?
- Have there been past efforts that were successful in compromising the facility's access control systems?
- Does the physical security system carry out assessments of alerts in the correct manner?
- Is there a minimal number of unnecessary alarms, including false alarms and nuisance alarms?
- Are there any spots along the perimeter where the cameras cannot detect an unlawful entry?
- When monitoring video surveillance systems, do security people or technological methods typically do the monitoring?
- Are the electronic security measures, such as intrusion detection systems, video surveillance, and other electronic security measures monitored locally or remotely?
- Do all the components that make up the video surveillance system (such as the video monitors, switching equipment, and transmission lines) work as they should?
- Does the lighting system work well in all respects?

3.6 VULNERABILITY ASSESSMENT: SECURITY SCANNING PROCESS

Willis (2022) proffers that vulnerability scanners are designed to identify previously discovered holes in a system's security and then offer instructions on resolving such issues. As a result of the frequency with which these vulnerabilities are published in public, a lot of information is currently available on software that is susceptible. Scanners that search for vulnerabilities in software and hardware in an organisation's infrastructure will utilise this information to locate susceptible hardware and software.

At first, the scanner will send probes to computers to determine which versions of software are running, which ports are open, which services are active, and which configuration choices are available. Vellani (2020: 76) indicates that the approach used for vulnerability assessment can be like that used for threat assessment, depending on the type of assessment performed, whether quantitative or qualitative in nature, and the type of matrix that is available. Imperva (2021: 39) points that the security scanning process consists of four steps: testing, analysis, assessment, and remediation.

3.6.1 Vulnerability Identification (testing)

The purpose of this stage is to compile an exhaustive inventory of all an application's flaws and weaknesses. According to Vellani (2020: 77), the vulnerability assessment is not yet being applied as part of an overall risk assessment in the first stage, and as a result, assets have not yet been identified. If the vulnerability analysis is going to be part of the risk analysis, then the information about the assets being evaluated should be readily available to the team doing the analysis. Scanning apps, servers, and other systems with automated tools or manually testing and assessing them to assess their level of security is one of the tasks performed by security analysts. Analysts also depend on vulnerability databases, vendor vulnerability notifications, asset management systems, and threat intelligence feeds when trying to locate security issues (Imperva, 2021: 39). Willis (2022: 22) believes that security practitioners can execute a vulnerability assessment with the right tools by first determining what they want to scan, which is not always as simple as it seems. However, with the right tools, they can complete the assessment. A lack of visibility into a department's digital infrastructure and the devices that are linked to it is one of the most prevalent and widespread difficulties that departments confront in terms of cyber security. All branches and levels of government provide its employees with mobile devices, such as cell phones, laptops, and other electronic tools that are able to regularly detach and reconnect with the workplace, as well as with employee residences and other off-site places (Willis, 2022: 36). The COVID-19 pandemic made the work-from-home approach available, which resulted in a significant increase in the number of vulnerabilities existing on the technological front and hence required investigation.

3.6.2 Vulnerability Analysis

Finding out where the vulnerabilities came from and what caused them is the objective of this stage, which came after discovering the vulnerabilities. Determining the components of the system that are accountable for each vulnerability as well as the underlying cause of the vulnerability is a necessary step in the process. An obsolete version of an open-source library, for instance, might be the root cause of a vulnerability. This outlines a distinct plan of action for the improvement or correction of (Imperva, 2021: 38). However, threat assessment is already in progress, and a review of the report ought to unearth any weaknesses that bad actors have exploited in the past. Consider the scenario described by Vellani (2020: 77) in which security staff reacted to an alert system from the same camera on many times. The occurrence was recorded in the threat assessment report.

The team that conducted the vulnerability assessment found out that the camera captures the facility's right rear perimeter fencing in its images. During the process, the group makes the startling discovery that the fence in that region is not only broken, but also of an older design than the fencing in the front of the facility (Vallani, 2020: 77). According to Mbanaso (2021: 39), vulnerability analysis in cyber security is the process of identifying and testing to determine current exposure, whether current security measures are sufficient in terms of confidentiality, integrity or availability, authenticity, non-repudiation, and trust. In other words, it is the process of determining whether current security measures are adequate. In addition, it shows whether the suggested safety controls would be sufficient.

3.6.3 Risk Assessment

Willis (2022: 23) opines that once the departments have evaluated the potential of harm, the next question is whether they can afford to do a vulnerability assessment on everything. They would do a vulnerability assessment on every system on a consistent basis if we lived in a perfect world. According to Vellani (2020: 77), this phase of the vulnerability assessment is meant to identify existing security measures for each asset and determine the effectiveness of each measure independently or in conjunction with others. Vellani argues that this phase of the assessment should be completed first. During their assessment of the facility, the team will locate and note on any site schematics or layouts any pre-existing security measures that are designed to close any known security holes. Depending on the facility and its security arrangements, the remedial measures may be evaluated in relation to established metrics and the department's standard operating procedures. When conducting a vulnerability assessment, one of the most common mistakes an assessment team might make is the assumption that existing countermeasures are adequate to combat the threat. The team will be able to establish whether the countermeasures are functioning as planned if they do performance testing. According to Imperva (2021: 30), the purpose of this phase is to rank the vulnerabilities in descending order of severity. It involves the security analysts vulnerability ranking or severity score in respect of the following factors:

1. the systems affected,
2. the information at risk,
3. the business functions that could be jeopardized,
4. ease of attack or compromise,
5. severity of the attack; and
6. potential damage caused by the vulnerability.

3.6.4 Remediation

Velleni (2020: 78) mentions that the team conducting the vulnerability assessment is required to produce a written report outlining the assessment and making recommendations for additional security measures or changes to the security programme to lower both the overall vulnerability and the vulnerability of specific assets. A fundamental cost-benefit analysis that outlines the potential for a lower degree of vulnerability to be attained because of applying the proposed security measures ought to also be included in the report. For critical facilities, the assessment team ought to take into consideration in their report the facility population, the structural integrity of the facilities, the land area of the facility, the distance to emergency services, redundant power supply, video surveillance systems, intrusion detection systems, barriers, outside lighting, and security guards. All these factors should be taken into consideration. Willis (2020: 25) agrees with Velleni (2020: 78) that an evaluation report is generated by the scanner once the vulnerability scan has been completed. When reading this report and developing remediation plans based on it, keep the following in mind:

- **Severity:** A vulnerability scanner should classify potential vulnerabilities according to their severity. When planning remediation, prioritise the most serious vulnerabilities first, but avoid ignoring the rest indefinitely. It is not common for hackers to combine several minor flaws to create an exploit. A good vulnerability scanner will recommend when to fix each issue.
- **Vulnerability Exposure:** As previously stated, not all vulnerabilities are on publicly accessible systems. Internet-facing systems are more likely to be exploited by any random attacker scanning the internet. Therefore, they should be addressed first. Furthermore, any employee laptops that have vulnerable software installed should be prioritised. Furthermore, any systems that host particularly sensitive data or could have a negative impact on that business might need to be prioritised over others.

Imperva (2021: 30) argues that the goal of this step is to close security gaps. Security, operations teams, and development typically collaborate to determine the most effective path for remediation or mitigation of each vulnerability. Specific corrective actions may include:

1. The implementation of new security procedures, measures, or tools;
2. Bringing operational or configuration changes up to date;
3. Creation and deployment of a vulnerability patch

Vulnerability assessment cannot be a one-time event. To be effective, departments have to operationalise and repeat this process on a regular basis. It is also critical to promote collaboration among security, operations, and development teams, a practice known as DevSecOps.

3.7 VULNERABILITY RATING SCALE

Vellani (2020: 78) indicates that the target's attractiveness and the level of protection provided assets is used to assign vulnerability ratings. A quantitative or qualitative rating scale can be used. The relative importance of qualitative ratings to the department's primary mandate is scaled. Quantitative costs are based on life cycle costs, which include the asset's actual value, replacement cost, operational costs, maintenance costs, and time lost while the asset is replaced or repaired. When employees lose their official vehicle, the department loses its current value, as well as the cost of purchasing a new vehicle and the cost of transportation between the vehicle's loss and replacement.

3.7.1 Scale of Qualitative Vulnerability

Vellani (2022: 78) presents the following is an example of a qualitative vulnerability rating scale for facilities:

Very High: A facility that has a history of threats, inadequate security measures, and adversaries that can exploit security holes. In the event of an assault on a facility of this kind, there is a possibility that the structure will be damaged, activities will be slowed down or brought to a total halt, and assets held within the facility will be lost.

High - A facility with tempting targets, no history of attacks, poor security measures, and opponents able to exploit security holes is considered to have a high risk. An assault on a facility of this kind may result in structural damage, limit activities to those that are necessary, and destroy assets that are housed within the facility.

Moderate: A facility with tempting targets, no history of threats, effective security measures, and no adversaries capable of exploiting security weaknesses; this level of threat is considered moderate. An assault on this kind of facility might not have much of an effect on the way things normally work.

Low: A facility that has no enticing targets, no history of threats, and effective security systems is considered to have a low danger level. Normal business will not be significantly disrupted in the event of an assault on this kind of facility.

3.7.1.1 Recommendations

Within the recommendations, part of the report on the vulnerability assessment are the proposed modifications to the security programme that were made by the assessment team. The deployment and redeployment of security personnel, the introduction of extra physical security measures, and the rewriting of security plans, rules, and procedures are all examples of potential alterations that might result from these changes. It is important that the suggestions be prioritised according to the vulnerability ratings assigned to each asset. This will enable security decision makers to modify appropriately that are suitable. In this portion of the report on the vulnerability assessment, a cost-benefit analysis and cost projections should also be included. Because budget requests need to be made, and expenses need to be justified, cost-benefit evaluations are very necessary. It is also possible to provide recommendations in phases, with an analysis of potential dangers and weak spots inserted in the gaps (Vellati, 2022: 85).

3.7.1.2 Appendices

The security managers should ensure that the report is easy to read and understand because the management of department are not experts in security, and that includes putting on the appendices. Appendices to the vulnerability assessment report may include blueprints, facility and area photographs, site diagrams, and floor plans. Include a copy of the security survey checklist and any cost-benefit analysis documentation for the reader's convenience. Vellati (2022: 85) proposes that the following vulnerability assessment report as shown in Table 3.1.

Table 3.1 Vulnerability assessment report outline

VULNERABILITY ASSESSMENT REPORT OUTLINE
Table of Contents
Executive Summary
Vulnerability assessment dates
Scope of assessment
Team composition
Facility characterisation
Critical asset description
Summary of threat assessment
Vulnerability assessment objectives
Summary of conclusions
Summary of recommendations
Background
Organisational mission
Criticality of the facility
Key staff
Major functions
Geographic location
Overall physical characteristics and conditions
Vulnerability Assessments 85
Significant features, including history
Occupant information
Community demographics
Supply chain and transportation system
Specific critical assets
Security policies and procedures
Regulatory and legal requirements
Reviewed facility blueprints, site diagrams, and floor plans
Identification of property boundaries
Location of authorised access points
Maps depicting facility ingress and egress paths
Descriptions of physical structures
Traffic patterns
Neighbouring facilities
Assessment overview & process
Identification of critical functions
Significant threats
Available documentation
Vulnerability assessment team composition and biographies
Schedule
Major vulnerability areas
Site
Environmental
Structural
Physical protection systems (PPS)
Policies and procedures
Documentation
Security plans
Security incident reports
Security personnel
Life safety and fire protection systems
Communications systems
Information technology security systems

Conclusions
Recommendations
Prioritised ranking of recommendations
Cost-benefit analysis of recommended changes
Appendices
Facility and area photographs
Blueprints
Site diagrams
Floor plans
Security survey checklist
Cost-benefit analysis documentation

A vulnerability assessment identifies the weak areas in a facility in relation to a particular risk. These vulnerabilities guide the process of accumulating security knowledge (Garcia, 2006: 1). Officers receive information on the types of crimes that are being committed thanks to a document called a Crime Pattern Analysis. It provides officers with information on any known suspects, suspect vehicles, *modus operandi,* and other property loss, as well as the dates, times, and locations where these occurrences took place (Govender, 2018: 192).

According to Govender (2018: 107), the most crucial aspect of a successful vulnerability assessment is accurately analysing the performance of the component that is being evaluated. This is accomplished by beginning with a performance value that has been tested for a specific component of a physical protection system such as a sensor, and then degrading the performance of the component based on the device’s installation, maintenance, testing, and integration into the overall system. This is done when taking a quantitative approach to solving the problem. For instance, if the sensor's performance value has already been tested, then the performance of the sensor will be worse after the testing. For qualitative analysis, the performance of each component is degraded in accordance with the same conditions. However, the device’s performance is assigned an effectiveness level, such as high, medium, or low, rather than a number. This is done so that the results can be interpreted more accurately.

3.8 PROBABILITY

After information on events, threats, and vulnerabilities has been collected and analysed, it is essential to assess the probability of loss using the information obtained (Govender, 2018: 107). When confronted with several issues, security managers are tasked with prioritising which of those concerns deserve immediate action. According to White (2014: 165), the purpose of the department's strategy to prevent crime, should be to minimise the chance of criminal activity to the lowest probability achievable. This aim may be achieved by the departments by taking a variety of actions, but the first step should be to identify the vulnerabilities and dangers that the departments are now facing. The following stage should be to investigate tried and tested preventative strategies, and the last step should be to put those preventative measures into action. Recognise that these measures will need to be updated over the course of time, and that the process should be assessed on an ongoing basis to ensure that it continues to be effective.

In most situations, a vulnerability analysis is included as a component of a more comprehensive security risk assessment. Combined, the two will frequently anticipate the efficiency of any suggested remedial activities based on the vulnerabilities that have been found. In addition, the final report should provide some insight into the results that can be anticipated once the suggestions have been put into action. If security holes are found during the process of conducting a security risk assessment, a comprehensive action plan should be formulated, outlining the steps to be taken and the changes to be made recommendations. In addition, the anticipated outcomes of those recommendations should be identified and documented. Security managers will assess a threat to a vulnerability based on the probability that an event would take place, although this will depend on the categorisation of the vulnerability. There is a level rating system in place for every discovery (White, 2014: 167).

3.9 IMPACT

Williams (2013: 53) indicates that a business continuity management process should be implemented using a combination of preventive and recovery controls to minimise the impact on the departments and recover from the loss of information assets that may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions to an acceptable level. This can be done to bring the situation back to an acceptable level. This process should identify critical business processes and integrate information security management requirements for business continuity with other continuity requirements for operations, resourcing, materials, transportation, and facilities. Additionally, this process should determine how to identify critical business processes.

According to Govender (2018: 108), to classify information on security events, threats, and vulnerabilities into more specific subcategories, security managers utilise criticality principles. The meaning of the phrase has been determined to be the result of a loss in rand. An estimation of the impact of the danger was created based on the departments' prior information as well as the experiences of departments that are comparable to their own that have been in circumstances that are comparable. Impact is often measured using the rand as the standard unit of measurement. The expense of replacement, repair, missed productivity, lost business opportunity, clean-up, litigation, reputational harm, and diminishing consumer goodwill are all factors that the security manager needs to take into consideration. Even when it comes to the value of human life, a rand value is the standard to use. Govender (2018: 108) states the following factors also have an impact:

a. Replacement cost (other indirect costs), The cost to replace such as indirect costs;
b. Temporary replacement (employment costs);
c. Interruption (not your usual business);
d. Reduced money (withdrawing money from the investment);
e. Changes in insurance rates (when the premiums go up); and
f. Taking advantage of market depreciation (unable to deliver the product timeously).

Govender (2018: 108) goes on to say that understanding the effect is an incredibly crucial notion for security managers. If the potential loss of money is larger than the cost of providing security, the management of the department, who often think in terms of cost analysis, will not be interested in spending money on security if the cost of providing protection is higher. Impact is a subjective measurement, much like likelihood, although it can be positioned anywhere along a continuum. Utilising the rankings that were generated for probability and impact, as well as developing a matrix system for various security risks, it is possible to quantify security risks to some extent and figure out which risks require immediate attention. This can be accomplished by creating a matrix for the various security risks. A probability and effect alphanumerical value may be provided to each security risk by using the matrix. If a decision has to be taken, the impact should be prioritised over the likelihood (Fisher, Halibozek & Green, 2008: 157-159).

3.10 SECURITY BREACHES

The proliferation of malware programmes and illegal access to the data that is housed in vital assets has made it extremely challenging to resolve the security breaches that have occurred involving sensitive information. Due to the fact that the risk appetite of each department is unique, it is imperative that the threat analysis tools be connected with the information security policy of the business in order to provide security controls at the departmental level. On the other hand, it has been observed that the current tools for threat assessment processes have not incorporated information security policy for effective security management (that is, confidentiality, integrity, and availability), which is based on the organisation's risk appetite and culture (Mbowe, Zlotnikova, Msanjila, & Oreku, 2014: 01). Mandell (2013: 15) argues that the Security Assessment will address the risk of a security breach in addition to preventing criminals from entering the building (Mandell 2013: 15). If the security of the departments is compromised, the security component setup will be in place to guarantee that a sufficient amount of evidence is acquired to assist in the investigation that will follow. According to Mahlatsi (2019: 06), in this day and age of information security breaches, the department needs highly developed strategic thinking on how to confront criminals who are highly talented and imaginative.

Grama (2011: 10) contends that the number of vulnerabilities is growing, and that there are problems in the way that the implementation of internal information security is carried out. The security flaw gives attackers the ability to identify workers and hack into their personal as well as professional accounts, which poses a threat to the security of the state. The Department of Digital, Culture, Media, and Sport (2019: 03) notes that in their research, the findings reveal that the consequences of breaches in cyber security might be substantial. Nevertheless, their qualitative findings show that, outside of the survey, the indirect, long-term, and intangible consequences of breaches, such as lost productivity or reputational harm, are typically disregarded. This indicates that departments, when they assess their approaches to cyber security, there is a possibility that they may underestimate the real cost and severity of breaches in cyber security. (Grama (2011: 10; Nkwana (2015: 4) makes a veiled reference to the fact that the level of security breaches and the publication of unauthorised information is exceptionally high, despite the departments' best attempts to manage confidentiality and integrity.

The MISS document (1998) indicates that heads of security or those tasked with an institution's security responsibility are required to report all instances of a breach of security, failure to comply with security measures, or conduct constituting a security risk as soon as possible to the NIA's Chief Directorate Security, and, where appropriate, to the SAPS (Crime Prevention Unit) or the SANDF. These reports should be made to the National Intelligence Agency's Chief Directorate Security (MI). In the event that there has been a breach of security involving government encryption, the South African Communication Security Agency (SACSA) should also be notified. The MISS paper from 1998 adds that whenever there is a breach in security, it is required to be reported using the procedures that are already in place. The head of the departments are the one who is accountable for seeing to it that all breaches in security are disclosed. Breach of security should always be handled with the utmost confidentially to protect the officer who was involved and to prevent the officer from being treated unjustly (South Africa, 1998).

3.11 SUMMARY

The chapter discussed vulnerability assessment in terms of threat assessment and cost effectiveness if implemented by service providers. It also considers how the outcome may influence which asset protection measures can be implemented or changed to reduce or eliminate any associated risks. The chapter discussed assessing the target's attractiveness in the event of an intentional attack, as well as the level of existing defences against various threats. Different types of vulnerability assessment were discussed to gain understanding of the tests performed and the scope of implementation was covered.

The following chapter focuses on risk assessment using the knowledge gained from vulnerability assessment. The risk assessment results will provide the STA project team with a risk profile of the departments. The risk profile reflects the departments' exposure to the measured risks and serves as the foundation for the next step in the process.

CHAPTER 4
RISK ASSESSMENT AND MANAGEMENT

4.1 INTRODUCTION

According to the ISO 27001/2, risk assessment is the “systematic consideration of the business harm likely to result from a security failure and the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented” (ISO, 2000). Security practitioners and managers look at security risk wholistically, so they perform risk management, risk identification, or risk assessment. However, risk presents itself in many different ways, so it is critical to take a broad view of risk to ensure that no critical categories are overlooked. As a result, various risk categories have been defined or listed as a kind of prompt or reminder to risk owners that there is financial, reputational, environmental, safety, strategic, project, and operational risk. For clarity, the researcher has categorised these risk types according to the study's underlying logic and framework.

The researcher is of the view that the same is true for risk categories, also known as layers or levels in a hierarchical system. When it comes to risk types, many security managers have different priorities, and they prioritise them based on their department's objectives. While considering major sources of risk, the study identified four major types of risks, which are technical risk, which varies depending on the type of government department. Then there is the financial risk, which varies depending on the business unit in charge of procurement. Then there's management risk, which includes internal departmental risks like how business units are structured, how management makes decisions, how they prioritise, and how management communicates policies and strategies to employees. Furthermore, management risk includes how resources are allocated. External risk is another major category that includes things that are outside of departments but have a direct impact on government's core business, such as regulatory authorities, laws, and politics.

The chapter commences with the concept of risk assessment and grouped the four categories as big headings in this chapter, which include Technical, Financial, Management, and External risks. This study further included the examination of vulnerability assessment.

4.2 RISK ASSESSMENT CONCEPT

Meloy and Hoffmann (2014: 08) point out that risk assessment is the outcome of a threat assessment, but the irony is that if it is conducted effectively, risk management is frequently modified according to the changing dynamics of the threat assessment, and the threat assessor is unable to know whether the subject would have become violent or not without intervention. The risk management component of risk analysis expands on the work of risk assessment by answering the questions: does anything need to be done about the risk? What can be done to remedy the situation? More importantly, what should be done about it? The STA distinguishes risk assessment and risk management as distinct and qualitatively distinct activities. While risk assessment is concerned with objective evidence to the greatest extent possible, risk management necessitates prudential judgments about which risks require management, the selection and application of treatment measures, and whether the dealings should be permitted. As a result, if there is uncertainty about risks during the investigation stage, the management measures chosen may be influenced (Commonwealth of Australia, 2005: iv).

Bickley (2017: 28) argues that the process of risk assessment starts with the identification of the numerous security risks that are present within a specific setting, as well as the ways in which the personnel, assets, programmes being executed, or departments may be exposed. After that, it analyses them with regard to likelihood and impact in order to ascertain the extent of the risk that is involved. Finally, it identifies and assesses the potential risk-management solutions that may be put into action in the organisation. According to Allen (2016: 56), a successful risk assessment or identification has to take place with the least amount of stress or interruption to the main operations of the departments involved. In order to effectively analyse or identify risks, there should also be monitoring and responsibility. In addition to this, a commitment should be made to ensure that the proper degree of protection and deterrent is in place for that firm. The objectives of the departments need to be specified before risks can be recognised and evaluated in respect to those objectives. In addition, each level of the department is responsible for defining its own goals.

Bickley (2017: 29) adds that once mitigating measures have been discovered, it is expected that some residual risk will remain. This residual risk should be compared to the risk threshold established by the department in order to assess whether or not the programme may continue. It is possible for a department to be found in violation of its duty of care if a risk assessment is carried out and measures are identified, but these measures are not put into practice. Documentation of the process of evaluating the potential threats to security is required, and this documentation should include both critical findings and suggested risk management strategies. The researcher disagrees with Bickley's (2017: 29) assertion that the final phase in the risk process is to identify and assess the many different risk-management methods that may be put into action. The researcher believes that the monitoring of such implementations and verifying compliance is the final phase in the process of security risk assessment. This step is also an ongoing process. The efficiency of several security systems is rarely monitored, even though numerous departments advocate for costly and intrusive enhancements in security.

When confronted with a particular danger, the management team in charge of security has a wide variety of risk reduction methods at their disposal. When weighing the various possibilities, one has to give significant weight to the question of which assets require protection in order to maximise cost efficiency. The ability to prioritise risk-reduction operations and respond to changing and emerging threats is afforded to security management by means of a thorough assessment of the potential security risks. Risk mitigation is a method for reducing the amount of hazard posed by an opponent. This can be accomplished by removing or intercepting the adversary before they launch an assault, limiting possibilities through increased security, or mitigating the repercussions of an attack that does succeed. Reducing threats, blocking opportunities, and lessening the impact of any adverse events are the three components of the optimal risk-mitigation approach, which unquestionably includes all three of them (Vellani, 2020: 19).

According to the researcher, determining which assets require protection should not be the responsibility of security management, but of a security committee comprised of representatives from all business units in the departments. The researcher maintains that effective information risk management extends beyond situational measures and that protecting departmental information is the responsibility of all employees who generate data in an official capacity or on behalf of the departments. On the other hand, the researcher agrees that security managers are the primary participants and driving forces behind information security performance. As a result, questions such as how to approach security decision-making, organise leadership, and integrate security into day-to-day business operations are actively being researched. The process of security risk assessment includes risk identification, risk analysis, risk evaluation, and risk treatment:

4.2.1 Identify Risks

During the risk identification process, the departments need to pinpoint the sources of risk, the regions of effect, the occurrences, and the reasons of those events, as well as the potential repercussions of those risks (Gruyter, 2021: 225). It is necessary to consider both the potential consequences of the identified hazards and their frequency of occurrence. Every business ought to establish a strategy that outlines potential dangers and specifies how each one will be addressed on an individual basis. In order for the departments to be effective if and when an event takes place, they need to maintain consistency while also changing preparations as required. In order for the project to be successful, the action plans need to be evaluated, and all of the project's stakeholders need to have a clear understanding of what is expected of them. As a direct consequence of this, the exposure to risk needs to be decreased (Allen, 2016: 59).

As requirements, the framework has to adhere to an agile mindset, be capable of diagnosing root cause (i.e., causal analysis), forecasting business impact, be adaptable to metrics programmes, and encourage cross-project reuse of risk knowledge. Such a solution should aid in the identification of risks based on historical data and the development of action plans to mitigate them (Gruyter, 2021: 102).

4.2.2 Analyse Risks

The process of analysing risks requires first gaining a grasp of the risks themselves. The results of a risk analysis are integrated into both the risk evaluation and the judgments on whether risks is be managed, as well as the risk treatment techniques and methods that are most suitable (Gruyter, 2021: 226). According to Allen (2016: 25), one of the key goals of security risk analysis is to give a more objective basis for the process that is being analysed. Every division ought to give some thought to the sorts of risk assessments that are pertinent to the goals that they have set. The management team's decision on the scope of the risk assessment is driven by their goals and objectives. It is possible for it to be limited and particular to a certain sector as well as danger (for example., financial, energy, transportation).

On the other hand, Gruyter (2021: 11) notes that risk analysis is often focused on finding things that may go wrong in the design and its development, which would result in a failure of the system. This is done in the context of an evaluation. The findings are distilled and reported in terms that top management and security managers can understand. This allows the findings to be fed into the risk management process, and managers can decide on risk action requests for treatments that can either mitigate risks or remove them entirely. If managerial choices are not essential, parties involved in the evaluation might come to an agreement on quick corrective steps.

According to Aven (2015: 3), the reliability requirement in this context refers to the extent to which the risk assessment produces the same results when the analysis is repeated, and the validity requirement refers to the extent to which the risk assessment describes the specific concepts that are being described. Both requirements are necessary for the risk assessment to be considered valid. Depending on how these criteria are used, the findings of risk assessments can be assigned varied degrees of "justification." Andales (2022) proposes a risk matrix that may be used as a tool for risk assessment together with other approaches and instruments. There is a wide variety of software and approaches that may be easily included into the operation of a company's process. The four risk assessment tools that are utilised the most frequently are the risk matrix, the decision tree, the failure modes and effects analysis, and the bowtie model. Some further approaches to risk assessment include the what-if analysis, the failure tree analysis, and the hazard operability analysis. The following presents how the risk matrix works:

Table 4.1: The functioning of the risk matrix

Likelihood		**Very**	**Likely**	**Unlikely**	**Highly Unlikely**
Consequences	Fatality	High	High	High	Medium
	Major Injuries	High	High	Medium	Medium
	Minor Injuries	High	Medium	Medium	Low
	Negligible Injuries	Medium	Medium	Low	Low

Source: Researcher's own illustration

During a risk assessment, a risk matrix is frequently used to measure the level of risk by considering the consequence/severity and likelihood of injury to a worker after being exposed to a hazard. The two measures can then be used to help determine the hazard's overall risk rating. When using a risk matrix, two key questions to ask are:

1. **Consequences:** How bad would the most severe harm be if exposed to the hazard?
2. **Likelihood:** How likely is the department to be aggressed if exposed to the hazard?

According to Andales (2022), the first question to ask when evaluating the consequences of a danger is, "If a worker is exposed to this hazard, how severe would the most likely serious injury be?" This is the question that should be asked when analysing the consequences of a hazard. For the sake of this consideration, it was believed that a risk and an injury are inescapable, and the only concern is with the degree to which the harm will affect the individual. In addition, while determining the probability, the question that ought to be asked is: *If the danger happens, what is the risk that the worker would be injured?*

It is important to differentiate between this and the probability that the risk will materialise. It is common to categorise the likelihood of a hazard causing worker injury as follows:

- **Very likely** – exposed to hazard continuously.
- **Likely** – exposed to hazard occasionally.
- **Unlikely** – could happen but only rarely.
- **Highly unlikely** – could happen, but probably never will.

4.2.3 Evaluate Risks

The results of the risk analysis are used as the basis for the risk evaluation's aim, which is to aid in making judgments about which risks require treatment and the priority order of treatment implementation (Gruyter, 2021: 226). Allen (2016: 28) alludes that people who oversee producing vulnerability assessments need to be taught to examine the impact of loss to analyse not just what happened but also how the danger impacts the departments. It is always vital to evaluate the impact of loss to the recognised vulnerability while doing an assessment of the potential hazards that might affect the departments. Allen (2016: 28) states that the following stage, which is to assess what countermeasures may be done to lessen or eliminate the possible danger based on the results of the risk analysis, is the next step in the process. Because each expense is scrutinized on a yearly basis, it is necessary to consider the cost of putting remedies into action. After then, the countermeasures need to be assessed to determine whether all the possible countermeasures have been put into action. The total risk reduction of the departments is influenced in some way by each of these criteria.

4.2.4 Treatment

The process of selecting one or more alternatives for altering risks and then putting those options into action is known as risk treatment. After being put into place, therapies either offer or alter the controls (Gruyter, 2021: 226). If the risks are dealt with in a piecemeal fashion, there is potential for friction and inefficiency. For example, this is normal practice in departments that deal with security and fire. Doors should be left unlocked if they are required for fire safety, but they should be secured if they are required for security. If one examines these dangers through the prism of overall operational risk management, one will be able to rank them in order of severity and deal with them as necessary. An overarching perspective can also help identify chances to treat numerous threats at the same time (Allen, 2016: 18).

Almost all the government departments are confronted with security risk, and they need to determine the exposure of such risk, and what are the consequences if such risk is not managed. The traditional definition of risk as "the likelihood and magnitude of an adverse event" appears incompatible with technical risk assessment.

4.2.5 Technical Risk

The magnitude of the difference between the actual and optimal design of product artifacts and processes, combined with uncertainty, is defined as technical risk. The definition provided here corresponds to practitioners' perspectives on technical risk. It allows for risk quantification and identifying potential product improvement areas (Antinyan, Staron, Sandberg & Hansson, 2014: 01). If technical risks are identified prior to operational phase planning, they can be defined as year zero (0) risks in a business model's levelized cost if they have an impact since the start of an operation, according to Moser, Del Buono, Jahn, Herz, Richter and De Brabandere (2017: 01). Only risks from year zero (0) are considered in this section. It is critical to understand how each of these risks' variability and associated uncertainty are calculated, as well as how the values are distributed in terms of probability. These variables are critical in determining the likelihood of exceeding and how it is influenced.

According to Hansson and Aven (2014: 17), technical risk refers to the potential impact of changes on a project, system, or entire infrastructure if an implementation does not go as planned. Failure to identify and manage these threats leads to decreased departmental performance, security breaches, system failures, increased maintenance time, and significant technical debt. To ensure early detection of these problems, it is critical to have a reliable analysis solution for technical risk management. This reduces the amount of effort required to address unexpected infrastructure or system problems and prevents problems from arising unexpectedly (Hansson & Aven, 2014*: 7)*.

Defence Science and Technology Organisation (DSTO) (2010: 01) states that the capabilities over existing systems can be improved using development technologies, this can further delay and cut costs. The developments of the Collins submarine indicate that an improved process of procurement and management of such developed systems, was recommended by the Department of Defence when they reviewed their objectives, including the technical risks that are inherited. DSTO (2010: 01) further indicated that the Defence Procurement Review 2003 (also known as the Kinnaird Review) recommended that the two-pass system for new acquisitions should be strengthened to include a "comprehensive analysis of technology, cost, and schedule risks." The Review also stated that the 'Government should be assured that adequate scrutiny is conducted by DSTO on technology feasibility, maturity, and overall technical risk.' As a result, the Chief Defence Scientist (CDS) was tasked with providing independent advice to the government on all acquisition decisions.

According to Antinyan, Staron, Sandberg, and Hansson (2014: 01), the challenges of technical risk assessment are difficult to address, but success can have a significant impact on software organisations. The main reason for this is the nature of an adverse event's outcome, which is more continuous than discrete. The study looks into various aspects of technical risks and provides a definition to help with risk assessment and management in software development.

4.3 SOFTWARE DEVELOPMENT

According to Giuffrida, Bardin, and Blanc (2018: 93), existing software defences, are ineffective. Given the difficulties in deploying hardware solutions, it is critical to develop effective software-based defences to protect mobile users from row hammer attacks. The authors conducted an in-depth investigation of the existing proposals, which can be broken down into two categories: those that aim to prevent attackers from triggering bit flips, and those that aim to make it impossible for a bit flip to render physical memory into an exploitable state. According to Giuffrida et al. (2018: 93), there are limitations in both directions. These limitations can be in terms of practicality, such as the fact that they require specific features of hardware, or they can be in terms of effectiveness, such as the fact that they still allow for row-hammer exploitation. Both limitations are problematic. They illustrate this inefficiency by introducing innovative assaults that exceed all defence mechanisms that have been devised and put into practice.

The resistance of programmes to malicious attacks that take advantage of flaws is one of the primary concerns of software security. On the other side, the requirements for security functions, such as authentication, may be stated as functional requirements. Increased connection and progress made toward the Internet of Things have both contributed to the development of new threats. In addition to flaws that have been found in traditional computer systems (such as the Heartbleed bug), flaws have also been found in devices and applications that are not often thought of as being particularly security sensitive. Some examples of these include vehicles and medical devices. In addition to this, the danger is no longer confined to major companies; small and medium-sized businesses are increasingly becoming the focus of cyberattacks (Assal & Chiasson, 2018: 281).

According to Gruyter (2021: 199), cloud computing companies who use a SaaS model are required to create, install, configure, and maintain the full infrastructure, platform, and applications stack to offer their clients with the specified service levels. Customers that use SaaS cloud services can access apps directly from a range of client devices by utilising interfaces such as web browsers (for example, Gmail and Yahoo! Mail) and an Internet connection to communicate with the cloud. One alternative moniker for the SaaS concept is the term "on-demand software services." Customers gain an advantage from using SaaS since they are only required to pay one set of expenses for license, installation, and maintenance. Customers using SaaS cloud services lose the capacity to exert control over the underlying cloud infrastructure, the platform, and even individual apps, which have restricted administrative access (Kavis, 2014).

Gruyter believes that cloud suppliers are accountable for the security of utilising a cloud, including the infrastructure, operating systems, and applications, as businesses move away from using in-house data centres and toward using cloud computing. Gruyter's argument can be found in Gruyter 2021:199. The degree to which consumers are responsible for maintaining a secure environment differs according to the cloud service models that are utilised by those customers. For instance, in an IaaS model, cloud suppliers oversee managing the infrastructure of cloud computing, which includes things like physical facilities, data centres, and network interfaces. PaaS models provide cloud suppliers additional obligations, such as managing operating systems and middleware, in addition to their existing ones. Customers using cloud services are still responsible for their own data safety and security, regardless of the models of cloud service used. In addition to this, it is always the customer's responsibility to ensure that the security needs are in accordance with the norms or standards of the industry (Chou, 2013). There is a high possibility of security breaches, which will result in monetary loss for the department if the security criteria are not completed in line with the department's security policy. If this is not the case, there is a high likelihood of security breaches.

4.4 FINANCIAL RISK

Monzon (2021) alluded that the International Business Machines (IBM) Security released the findings of a recent study, which found that data breaches now cost South African businesses $3 million (R46 million) on average – the highest cost in the report's 6-year history. The average financial damages arising from a data breach increased by 10% year over year, reaching $4.24 million in 2021. Based on an in-depth analysis of real-world data breaches experienced by South African departments, the study concludes that security incidents became more costly and difficult to contain because of drastic operational shifts during the pandemic, with costs rising 15% for South Africans compared to the previous year.

Lohrmann (2021) indicates according to that the IBM and the Ponemon Institute report (2021), the average cost of a data breach among surveyed companies reached $4.24 million per incident in 2021, the highest in 17 years. Here are some more compelling statistics:

- The impact of remote work: The pandemic presented a unique challenge for both private and government department which resulted into a rapid shift to work remotely, and the outcome become more expensive due to data breaches. When the operations became remotely, breaches cost over than a million dollar on average than those in this group who did not have this factor ($4.96 vs. $3.89 million);
- Costs arising from health-care breaches increased radically: Institutions that made important changes in their operations due to the pandemic, such as hospitals and health care centres, to a huge increase in loss of information costs year over year. The departments that suffered most in breaches are health care centres, with a $2 million increase over the previous year, costing $9.23 million per incident;
- Compromised credentials resulted in compromised data: The study found that stolen user credentials were the most common root cause of breaches;
- Most breaches derived from loss of user credentials, in addition, the personal data of the customers were exposed and information such as names, emails, and passwords were stolen. The breaches reported by the study accounted to 44 percent of all breaches; and
- The three factors of mitigations that were recommended for reduction of cost of security breaches included security analytics, adoption of AI, and encryption. Companies saved between $1.25 million and $1.49 million when compared to those who did not use these tools at all. For cloud-based data breaches studied, departments that used a hybrid cloud approach had lower data breach costs ($3.61 million) than those that used a primarily public cloud approach ($4.8 million) or a primarily private cloud approach ($4.55 million).

Allen (2016: 31) asserts that when it comes to upgrading products and putting in place new programmes, cost is always an essential factor to consider. One example of this is the installation of security systems. One example of this is the necessary number of security guards for the departments. The annual expense of maintaining the status quo regarding these workers will very probably go up. There are times when it is necessary to consider reducing the number of employees and replacing them with a more cost-effective option. In a similar vein, evaluation of the equipment should consider both the cost and its dependability. It is possible that modern security systems are more or less expensive than previous ones, but the most important thing is to prioritise reliability, adequate employee and asset safety, and effective risk management.

4.5 MANAGEMENT RISK

Gruyter (2021:181) makes a passing mention to the fact that risk management is an ongoing effort. The use of risk-based security helps to strike a balance between the expanding number of security risks and the ever-increasing complexity of the life cycle. In contrast to many other initiatives that came before it, research and various practice projects have shown that designing for security is beneficial but not adequate on its own. For security to be successful, it is necessary to cover all stages of the life cycle. It is essential to include security early in the design process in order to gain an understanding of the dangers and hazards posed by embedded functionalities.

According to the ISC (2016: 53), a holistic strategy to distributing resources is the best way to safeguard a facility, its assets, and its people while yet maintaining an acceptable level of risk. The decisions that are made on risk management are based on risk assessments, risk mitigation, and risk acceptance, if required. An expanded definition of risk management is the act of recognizing, analysing, and communicating risk to accept, avoid, transfer, or control it to an acceptable level at an acceptable cost. This definition is based on the idea that risk may be managed in several ways. According to the ISC (2016: 53), the primary objective of risk management is to limit or eliminate risk by means of mitigation measures (preventing the risk or reducing the risk's negative impact). However, risk management also includes the concepts of risk acceptance and/or transfer depending on the circumstances. The ideas behind risk management acknowledge that while risk cannot always be avoided, it can always be mitigated.

There are a number of challenges that have to be overcome in order to effectively manage risks, some of which are listed below according to Williams (2017: 2):

- A lack of integration, in which risk management is utilised as an add-on rather than integrated with other management processes, or if there is a "silo" approach rather than a strategy approach at the departmental level, both of these issues
- An absence of a systematic approach, which frequently results from the flawed belief that risk management is automatically ingrained in day-to-day decisions, as well as an absence of clear reporting to senior management and the audit committee, which typically accompanies this deficiency, are two of the most common causes of this weakness.
- An abdication of responsibility brought on by individuals' lack of interest in or awareness of risk, which can be brought on by poorly written job descriptions and a weak or absent risk management process; and
- A lack of risk connectivity between the top and bottom levels of the department;

In South Africa, most senior position in the departments is politized and people without academic qualifications are appointed on senior positions. The above-mentioned management risk mentioned by Williams (2017: 2) outlines how the security of the departments can be compromised due to lack of good management who cannot develop good policies and Standard Operation Procedures (SOP).

4.5.1 Policies and Standard Operation Procedures

Risk is often quantified in terms of likelihood and consequence, according to the Australian Fisheries Management Authority (2019: 04). Risk is defined as the influence of uncertainty on an aim. Effective risk management requires the methodical implementation of management policies, practices, and procedures to the activities of consulting, establishing the context, communicating, as well as identifying, monitoring, analysing, treating, evaluating, and reviewing risk. These activities include communicating, consulting, and establishing the context; establishing the context; and identifying, analysing, evaluating, treating, monitoring, and reviewing risk. It is broken down into four primary steps, which are risk context, risk assessment, risk treatment, and risk monitoring. Consultation is carried out during each stage. The purpose of the process of risk assessment is to offer insight into the potential sources of risk and the potential repercussions, as well as to act in the event that unfavourable outcomes or hazards occur.

Williams (2013: ix) alludes to the fact that the purpose of developing comprehensive security policies is to that satisfies the needs of the departments, using compliance standards as a guide to ensure that our security policy satisfies the requirements of the various standards. In this regard, the following statements are designed to elicit comments from management in order to construct an information security policy document that integrates the various needs of the various standards. The researcher contends that it is very difficult to design a cyber security strategy that would be proactive and will be embraced by management in the public sector, particularly in the government. It is difficult for the management in the departments to differentiate between cyber security and digital forensic investigation, which has a direct influence on the process of establishing cyber security as a function. Sets of security policies should cover many of the same concerns; however, the level of control, the severity of the penalty, and the degree of supervision in these policies should be adjusted to the department's threat environment, the industry, and the business culture (Landoll, 2016: 6).

Bayuk, Healey, Rohmeyer, Sachs, Schmidt and Weiss (2012: 3) assert that cyber security policy addresses the conflict between demand for cyber functionality and security requirements. The term "policy" is used to describe a variety of cyber security situations. It has been applied to laws and regulations governing information distribution, private enterprise goals for information security, computer operations methods for controlling technology, and configuration variables in electronic devices. In general, "cyber security policy" refers to directives intended to maintain cyber security.

Allen (2016: 31) mentions that any security programme should have policies and procedures in place that are cost-effective. To ensure that financial goals are met, every effort should be expended to review available resources. Manpower, hardware, and technology are examples of resources. Each has to be evaluated in terms of what is best and most cost-effective for the department. In addition, Allen (2016: 33) points at one approach that can determine whether a security survey is required as to focus on available security services for the particular needs of the departments. The security survey can aid the departments in determining the effectiveness of their security plan, and whether it is sufficient to meet the needs of the departments. The security plans are not meant to meet the needs of the departments wholistically, but to focus on the specific needs. Therefore, establishment of security policies and procedures will aid in determining policy contradiction or formulates policies that would complement one another, and whether there is need to for consolidation. These policies have to be renewed every year to ensure its effectiveness and appropriateness for current challenges such as cybersecurity strategy.

4.5.2 Cybersecurity Strategy

Masombuka, Grobler and Duvenage (2021: 285) state that the South African government's pursuit of widespread internet access, its growing use and reliance on digital services, and the emergence of new technologies has given rise to new cyberthreat threats and risks. This is because the government is pursuing widespread internet access at a time when new technologies are emerging. A coordinated effort involving all levels of government is required for there to be any hope of developing a successful cybersecurity strategy to address these threats. On the other hand, taking a disproportional approach to cyber security seems to be necessary in light of the fact that the government is structured on three levels: national, provincial, and local.

According to Masombuka et al. (2021: 285), it is essential that cybersecurity on the provincial and local levels be prioritised, resourced, and tailored to their respective functions. However, this should not be done at the expense of underestimating the significance of cybersecurity on the national level. The circumstances in which the activities of national, provincial, and municipal governments are carried out are different from those of the national government, despite the fact that there are certain commonalities across these domains. As a direct consequence of this, the one-size-fits-all strategy to cybersecurity adopted by the national government is neither properly inclusive nor truly downward scalable. The continued growth of cyberspace and the challenges that it poses requires a contemporaneous and continuous adaptation in the methods that are used to construct resilient cybersecurity at all levels of government. This is required because cyberspace is always changing and posing new threats. In the event that this does not occur, local government in particular will continue to be an alluring target and a weak point in the cybersecurity defences of the government.

Gercke (2014: 12) indicates that the departments utilise a wide array of cutting-edge technologies and methods to protect essential corporate assets. Trust, on the other hand, is the single most crucial component of any cybersecurity programme. It acts as the basis for all the decisions that senior management makes about tools, talent, and procedures. On the other hand, according to their views, there is a widespread lack of trust in the cybersecurity initiatives of many departments because of conflicting goals. However, the chief security officer and his team prioritise security on a daily basis since even the most ordinary internet transactions provide weaknesses that may be exploited. Senior business executives and the board may only address cybersecurity after an attack happens.

This lack of trust, according to Choi et al. (2017: 9), is what causes common misconceptions about cybersecurity, such as the types of threats that are the most relevant, the amount of money that is required to protect critical information, and even which data sets are the most susceptible to being compromised. When beliefs are accepted as truth, the level of trust between parties continues to erode, and cybersecurity initiatives are unable to reach their full potential. If, for example, the number of data breaches that have occurred has been low, business leaders may be tempted to reduce the amount of money allocated to cybersecurity until the chief information officer (CIO) or other cybersecurity leaders demonstrate the need for additional investment in controls. This could potentially leave them open to an attack. In contrast, if threats are frequently documented, business leaders may make rash decisions to overspend on new technologies without realizing that there are other, nontechnical solutions to keep data and other corporate assets safe. These decisions may be made without realizing that there are other, nontechnical solutions to keep data and other corporate assets safe.

According to Goldstein, Hogan-Burney and Manky (2020: 6), an estimated 4.66 billion people worldwide use the internet nowadays, a figure that has tripled in the last 12 years as connectivity has become more widely available and will continue to rise. The reliance on computers and technology has altered the way we conduct business, communicate, and socialize, and technology is now an essential component of all aspects of life. Humans are becoming increasingly reliant on the internet, but our efforts to protect people, data, devices, and the internet's infrastructure from cybercriminals have fallen short of the threat they pose. Cyber criminals steal an estimated $600 billion per year from governments, businesses, and individuals, with the total loss of company revenues expected to reach $5.2 trillion over the next five years, from 2019 to 2023. Cybercrime, in fact, is one of the most disruptive and economically damaging criminal activities. Not only does it cause significant financial damage and pose a serious threat to society and the global economy, but it also has indirect consequences by undermining public trust in digital transformation and overall trust in technology.

Hansson and Aven (2014: 18) state that the idea that some assets are especially vital to a company's existence has to be at the core of an effective cyber-security plan in order for it to be successful. Because in our increasingly digitalized world, safeguarding everything in the same manner is no longer a viable choice. On the other hand, trust is very essential to the operation of the digital business model. If there is not enough security at the client interface, the risk might become existential. Over the past five years, the number of both small and big system breaches, as well as the sophistication and complexity of the assaults, have more than doubled. Even though they are aware that their defences will not be able to keep up with future attacks, most large departments continue to address the problem as a technological and control issue. This is even though they are aware of the seriousness of the situation. In addition, these defences are typically conceived with the intention of safeguarding the outskirts of corporate activities and are implemented in a manner that is inconsistent throughout the various divisions of the company. The researcher agrees with the authors that the next wave of innovation in customer applications, business processes, technology structures, and cybersecurity defences should be founded on a business and technical strategy that places a priority on the protection of critical information assets. This technique is known as "digital resilience," and is a cross-functional strategy that identifies and analyses all risks, establishes enterprise-wide goals, and determines how to fulfil those goals in the most effective manner (Hansson & Aven, 2014: 18).

Management formerly had the ability to engage lengthy and in-depth conversations about technological strategy without ever bringing up the subject of security (Gercke, 2014: 12). Even if cybercriminals are becoming more clever and able to adapt to various defences, departments in recent times have enormous assets and value that are manifested in digital form, and they are strongly tied to global technological networks. Most government agencies, committees, and top executives are aware of the grave dangers that cyberattacks represent to the operations at the centre of government. What they do not know is how to establish a plan that will help them comprehend and deal with dangers in all of their guises, both in the present and in the future. This is something about which they are concerned. In addition, they require such a plan daily.

On the other hand, the experience gained while working to defend some of the largest and most technologically advanced corporations in the world has revealed three overarching requirements that can aid departments in updating their efforts regarding cyber security. They give an exhaustive series of articles inside this compendium that detail how departments may make these demands a reality and assist their leaders in getting a better night's sleep as a result. Based on his years of experience working in the field, the researcher agrees that an effective cybersecurity strategy offers differentiated protection for the organisation's most valuable assets through the implementation of a collection of security measures that are arranged in tiers (Garg, 2020: 9).

In recent times, the principal targets of cyberattacks were governmental organisations and financial institutions (Garg, 2020: 9). The danger is now on a worldwide scale as a result of every organisation linking an increasing number of their activities to the internet. Think about the destruction that was brought about by these three recent incidents. Between the years 2011 and 2014, the cyberespionage organisation known as ‘Dragonfly’ targeted energy businesses located in the United States of America, Europe, and Canada. In the month of May 2017, the WannaCry ransomware seized public and commercial companies in the fields of telecommunications, healthcare, and logistics hostage. During the same year, the ransomware attacked several large organisations in Europe that were in a variety of different industries. Meltdown and Spectre were discovered to be two of the most dangerous cyberthreats ever in 2018, indicating that vulnerabilities are present not just in software but also in hardware. Meltdown and Spectre were discovered in 2018.

Bailey, Kolo, Rajagopalan and Ware (2018: 34) point that one of the most significant unresolved issues in cybersecurity is insider threat via the departments' own employees, as well as contractors and vendors. According to a recent study, it is present in 50% of reported breaches, the departments are aware of the issue, but they sparsely devote the resources or executive attention required to solve it. Most prevention programmes fall short, either by focusing solely on monitoring behaviour or by failing to take cultural and privacy norms into account. The researcher concurs with Bailey, Kolo, Rajagopalan and Ware (2018: 34), that there is no sense of accountability and the departments aware of perpetrators, but no one is getting charged or arrested for security breach. Bailey at al state that some of the world's leading companies are now experimenting with a micro segmentation approach to target potential problems more precisely. Others are implementing extensive cultural change and predictive analytics. These new approaches can produce more accurate results than traditional monitoring and can also assist businesses in navigating the tricky business of protecting assets while also respecting employees' rights.

Bailey et al. (2018: 34) further state that the departments sometimes struggle to define the term "insider threat." This term is used to refer to the cyber-risk posed to departments as a result of the rather than other types of behaviour of its employees’ harassment, workplace violence, and other insider threats are examples of insider threats. or wrongdoing Contractors and subcontractors are used for this purpose. Many vendors are also considered employees. The largest cases in recent memory have relied on third parties. parties at their heart Inside threats are created by two types of employees: those who are negligent and those who have malicious intent. departments can easily understand negligent or co-opted insiders; through poor training, low morale, or pure carelessness, normally reliable employees can expose the company to external risks. Departments, on the other hand, frequently misunderstand malicious insiders in two ways.

Goldstein, Hogan-Burney and Manky (2020: 3) state that governments have traditionally been in charge of combating crime. However, the unique realm of cyberspace has demonstrated that governments do not and will not have all of the capabilities required to combat the cybercrime threat on their own. Indeed, many of the required capabilities are found in the private sector, so private companies have to be included in the solution. Enabling stronger operational collaboration between the private and public sectors on a global scale, as well as combining their resources and capabilities, are thus critical elements in mitigating the risk posed by cybercrime. There are numerous significant collaborative initiatives, but they are fragmented and insufficient for current needs. As a result, there has been a change in basic assumptions in how these challenges should be addressed collectively through security structured communication.

4.5.3 Communication

Communication and consultation occur at all risk management process levels between those in charge of risk management implementation and those with own vested interests. This provides insight into how decisions are made and why certain treatments are required. Instead of a one-way flow of information from decision-makers to stakeholders, the emphasis should be on consultation (AFMA, 2019: 05). Unlike in the militant approach of command and control that is used in the SANDF and SAPS, modern managers understands that field workers are in the position to know the threat picture that the departments are facing, and the best way is to consult with them before they implement security measures. Most departments employ specialists on the level entry, and they expect them advice management on improvement of security features. All this requires precise communication between the management, sub-ordinates, and the stakeholders.

Harbach et al. (2014: 33) state that communicating the risk associated with specific actions has long been a concern in human-computer interactions. A substantial amount of previous research has focused on how to effectively communicate security risks in general, such as those caused by insecure SSL connections or phishing. Many IT security systems employ a decision dialogue to inform the user about potential risks or privacy implications. Recent research, however, has repeatedly demonstrated that such dialogues are frequently ineffective and quickly ignored, or provide information that is difficult for the user to understand. in comparison, Rader, Wash and Brooks (2012) indicate that informal stories have an impact on security behaviour and thinking as they are passed down from one user to the next. These stories provide concrete examples of good and bad things that have happened to people that a user can relate to. Previously, Blackwell, Church and Green (2008), proposed that abstract information in software creates a schism between system designers and users.

Hull (2018: 637) indicates that preventing employees from engaging in inappropriate behaviour is critical for departments, because it can be very costly in terms of regulatory fines, legal costs, and reputation. Some innovations enable businesses to track their employees' conversations across multiple communication platforms. For example, Digital Reasoning, a Nashville-based company with offices in London, New York, and Washington, has developed surveillance software that is used by some of the world's largest banks and asset management firms (Council of Europe, 2001: 2). It can listen in on English conversations (handling six different dialects). Hull (2018: 637) adds that it can monitor employee behaviour by analysing millions of e-mails, chat logs, and phone conversations to detect suspicious or unusual activity using machine learning. If machine learning detects an employee whose behaviour deviates significantly from the norm, further investigation may be necessary. In an asset management firm, the behaviour could be indicative of insider trading, which, if allowed to continue, could result in a large fine. In a financial institution, it could be indicative of rogue trading or a failure to treat subordinates with respect.

Ebert (2021: 164) state that information security is the sum of all characteristics of an information system or product that contribute to ensuring that information processing, storage, and communication protects integrity, availability, and trust. Information security implies that the product will not do anything with the processed or managed data that is not explicitly stated in its specifications. Williams (2013: 32) argues that the sensitivity and criticality of information vary. Some items may necessitate additional safeguards or special handling. To define an appropriate set of protection levels and communicate the need for special handling measures, an information classification scheme should be used. If sensitive or classified information from the department falls into the hands of unauthorised people, aggressors, or the media, it has the potential to ruin the department's reputation.

4.5.4 Reputational risk

Reputational risk is defined as risk arising from negative customer perceptions on the part of counterparties, customers, investors, shareholders, market analyst, debtholders, other relevant parties, or regulators that could negatively affect a department's ability to maintain existing or establish new business relationships and continue access to sources of funding (BIS, 2009: 19). If communication and disclosure effectiveness play an important role in the process, the usefulness of environmental management and reporting as a hedging instrument for reputational risk is addressed through various levels of information transparency. When considering a voluntary reporting scenario, it shows that environmentally conscious departments can reduce the cost of environmental management as a reputational risk strategy while also reducing the potential loss of reputational value from reputational threats and increasing the potential revenue from reputational opportunities.

Hull (2018: 587) indicates that the risk of loss arising from insufficient or failed internal processes, people, and systems, or external events. Model risk and legal risk are included in operational risk, but risk arising from strategic decisions and reputational risk are not. The researcher argues that the departments should include the reputational risk in their risk model. This procedure entails conducting a thorough pre-employment screening to avoid hiring people with a bad reputation. With some of the experienced people who were involved in corruption scandals such as the "State Capture Commission" and the “Venda Building Society/ VBS bank scandal" now applying for senior positions in the departments, this can give the departments a bad reputation. Nobanee, Alhajjar, Abushairah and Al Harbi (2021: 2) indicate that the most valuable commodity in modern business is reputation, and this is the same in government department. The department with a good reputation creates market satisfaction, employs, and retains high skilled professionals. It further establishes a long-term relationship with stakeholders and investors.

Lemke and Petersen (2013: 413) argue that professionals in the supply chain context manage a variety of risks that have the potential to disrupt supplies. Surprisingly, one type of risk is frequently ignored: reputational risk. It is critical to recognise the risk potential that has an impact on the departments' reputation. Managers will also need an appropriate tool set to control it. Management builds a good reputation when they do a good job, and this has a positive impact on the departments and their stakeholders. This enhances the department's image, attracts more resources, and improves performance. As a result, there is no single correlation between corporate social performance and corporate financial performance. The activities that generate social performance have no direct impact on the department's financial performance, but they do have an impact on intangible assets. The departments should adjust their risk management methods and different response will be required for external risk.

4.6 EXTERNAL RISK

Hull (2018: 517) states that there is a different between internal and external risks. Internal risks are those that are under the company's control. The company decides *who* to hire, the computer systems to develop, the controls to put in place, and so on. Some people consider operational risks to include all internal risks. Operational risk then encompasses more than just the risk associated with operations. It includes risks associated with insufficient controls, such as the rogue trader risk and the risks associated with other types of employee fraud. Hull (2018: 517) adds that it includes the effect of external events such as natural disasters (for example, a fire or an earthquake that disrupts the operations of the departments), political and regulatory risk (for example, being barred from operating in a foreign country by the government of that country), security breaches, and so on.

Meloy and Hoffmann (2014: 74) state that the department should have laws that used to keep aggressors away from potential victims during high-risk periods of vulnerability, confine them for treatment, impose external behavioural control, and establish structure after release. The researcher believes that because the STA is proactive, it can be effective in identifying dangerous behaviour among employees; however, vulnerability assessment should be included as part of the process.

4.7 MITIGATION

The risks, vulnerabilities, consequences, and mitigation measures will vary and should be considered from an in-out perspective. At the intersection, there is an opportunity to mitigate risk and prevent threat from becoming reality. Law enforcement agencies can be human or nonhuman in the pragmatic of resilient countermeasures derived from analytic tools, risk management processes, technological, or other human instruments originating from internal or external sources. As a base, the conceptual framework could be reordered to be sources, mediums, perpetrators, intent, enforcers, and consequences (Thompson, 2019: 4).

Gruyter (2021: xii) indicates that Mitigation principles and practices that are specific to each situation make this a complex topic with numerous implications. The emphasis is not always on avoiding and reducing risks, but on knowing when and how to embrace risk to increase the probabilities of project and the success of the department. Allen (2016: 61) argues that the mitigation strategies are based on the asset's value in relation to the threat, vulnerability, or both. Risk is also determined by the probability of an event occurring. On each level, the risk assessment compares the threat and asset value to the identified vulnerabilities. Furthermore, Allen (2016: 61) states that for the departments to evaluate mitigation measures, the security managers should calculate the risk based on how the mitigation measures are used and whether they affect the value of vulnerability assets. Each mitigation measure should be weighed against the risk. The final phase is to determine which mitigation measures will be provide the departments with the greatest reduction at the lowest possible cost, by performing a cost benefits analysis.

According to Mbanaso (2021: 43), cybersecurity risk mitigation refers to activities such as policies, processes, and technical controls embedded in cybersecurity governance by the departments to help prevent security incidents and data breaches while also limiting the extent of damage when security attacks do occur. Thompson (2019: 31) admits that Mitigation is difficult; even money cannot be a quick fix; a deeper level of transformation may be required. Computers and systems should not be managed like property because layering new technology on top of old technology frequently means that security cannot be achieved because standard configurations should be modified to adapt to the new technology (Rogers, 2008: 14). When this change is made, both remote and in-person monitoring of intrusions becomes extremely difficult. More investment is required to keep standard configurations up to date with the most recent software, as well as extremely frequent scanning and full vulnerability patching.

4.8 MONITOR THE IMPLEMENTATION

Gruyter (2021: 67) posits that the implementation phase refers to putting the chosen course of action into action and monitoring its outcomes. Finally, the learning phase denotes a post-mortem examination of the implemented decision, its expected and actual outcomes. Gruyter (2021: 67) mentions that the relevant risk monitoring and evaluation activity, as well as the use of descriptive analytics tools, have been nonexistent. Given that the main purpose of risk monitoring and evaluation is to track software project health status via risk tracking to timely identify critical deviations from projected plans and apply the appropriate corrective actions, this identified situation opens significant research opportunities. Dashboards and visualization techniques provided by descriptive Analytics tools naturally support this tracking and monitoring activity. Allen (2016: 57) concurs with Gruyter (2021: 67) that the departments should put in place the necessary tools to detect and address potential risks before they occur. A controlled environment makes it easier to identify potential risks. However, for departments to be effective, risk exposures have to be continuously monitored.

Allen (2016: 85) states that when the physical threat monitoring system is applied, the departments should deploy sensors in sensitive areas and along likely attack channels, collect all available information that can assist in identifying the specific problem, and create a system that can aggregate this information and distil it into important details that should be acted upon. Ongoing monitoring is a critical component of model validation. This includes the testing and documentation of all model changes. In the event that the model user and model developer are the same person (as is sometimes the case) the model user may be tempted to modify the code to ensure the performance of the model is improved (Hull, 2018: 571). Policy should be rooted in some meaningful doctrine purpose, have a nexus to a law or regulation, or be tied in with or be about the Accounting Officer's vision, accountability to stakeholders, or the department's primary mandate; all should be directly linked in with the it's values and be strategically conveyed. it should be remembered that if the departments have employed credible people through the proper human resources' procedures, policy should be easier to follow; however, monitoring should never be omitted (Thompson, 2019: 64). If the vulnerabilities are not mitigated or monitored effectively, the departments would experience the security breaches.

4.9 SUMMARY

The chapter defined risk assessment as concept and further categorised the types of risk as heading to structure the chapter. The chapter discussed the technical, financial, management, and external risks. The chapter discussed security breaches as well as the installation of security components to aid in the subsequent investigation. The principles and practices of mitigation strategy were discussed. The chapter further discussed in the balance of probabilities; the cost effectiveness is an important factor in determining which assets require protection, and as a comprehensive security risk assessment that enables security management to prioritise risk-reduction activities and conform to varying and emerging threats.

The chapter also discussed various risks, vulnerabilities, consequences, and mitigation measures that should be considered from an in-out perspective. It further identified opportunities that can be used to mitigate risk and prevent threats from becoming reality.

The next chapter focuses on the legal mandate and policy documents that support the implementation of security programmes in government departments. The chapter further addresses the decided cased on selected legislations.

CHAPTER 5
LEGAL MANDATE

5.1 INTRODUCTION

The security component in all government departments should develop and implement security programmes that support the primary mandate of these departments and ensure that policy documents relate to their mission and vision (Williams, 2017: 12). Moreover, the formulation of security policies should be in line with the legislations and national policy document, namely, the Minimum Information Security Standard. This chapter commences with the highest law in the land, the Constitution of the Republic of South Africa, 1996, and integrates related case law in discussing the legislations. Furthermore, the chapter focuses on supplementary legislations and policy documents that support the implementation of security threat assessment. The chapter further addresses the Canadian laws on security privacy and challenges that they face on cyber security.

5.2 THE CONSTITUTION OF THE REPUBLIC OF SOUTH AFRICA, 1996

In order to execute the functions of national security, the Constitution of the Republic of South Africa, 1996 enacted the National Strategic Intelligence Act No. 39 of 1994. This piece of national legislation authorises certain government agencies to maintain an intelligence collection capability. According to De Kock (2011), the SAPS has a criminal intelligence unit that is responsible for gathering intelligence for the purpose of policing. The SANDF is in charge of Defence Intelligence, and the SSA is responsible for gathering intelligence for all other government ministries. According to Govender (2018: 107), the legislation does not include provisions for private security. The researcher is of the view that this particular piece of legislation is quite effective, in contrast to the three intelligence bodies, which are not. The function of these intelligence agencies is to identify potential dangers before they materialise, but they were unable to do so in the case of the looting in KwaZulu-Natal that occurred in 2021. In addition, the fire that broke out on South Africa's Constitutional Hill brought the nation's security establishment into disrepute, and left questions concerning the capabilities of intelligence agencies in South Africa.

On the other hand, employees frequently complain about how the security and intelligence violates their privacy. Chapter 2 of the Constitution of the Republic of South Africa (1996), also known as the Bill of Rights, states that the people shall be treated with democratic values such as human dignity, equality, and freedom. On the other hand, employees frequently complain about how the security and intelligence violates their privacy. The rights outlined in the Bill of Rights are ones that the state is obligated to respect, defend, promote, and fulfil. However, the Bill goes on to state that the rights are subject to the limits that are mentioned in Section 36 or anywhere else in the Bill. These limitations can be found anywhere in the Bill. Employees have a constitutional right to work in conditions that are safe for them, where their lives and personal information are protected, and where they are able to carry out their jobs without fear of reprisal. When they are on the premises of the departments, security managers should be aware that employees and visitors have the right to have their inherent dignity respected and that they have the right to be safeguarded from harm.

5.3 PROTECTION OF INFORMATION ACT, 1982 (ACT NO 84 OF 1982)

The revelation of information that should be protected is prohibited by Section 4 of the Protection of Information Act 84 of 1982; however, this provision is in conflict with the constitutional provisions that relate to presumptions. The Act does not include any provisions for the establishment of standards for the presentation of government information in legal proceedings. In addition, it does not include any relevant offences or minimum sentences for those who commit crimes (South Africa, 1980).

5.3.1 Council of Review, South African Defense Force

In the matter between the Council of Review, South African Defense Force (first appellant), Brigadier A. K. de Jager in his capacity as the confirming authority in respect of the court martial of respondents, held at Cape Town in January 1988 (second appellant), Colonel M. Dempers (third appellant), and Heinrich Johannes Monnig (fourth appellant), Case No. 610/89 was heard in the Appellate Division of the Supreme Court of South Africa (first respondent). Pieter Reinhard Pluddeman (second respondent) William Desmond Desmond Thompson (third respondent) Coram: Corbett CJ, Van Heerden, F H Grosskopf, Nienaber, JJA et Preiss AJA The date of the hearing was November 15th, 1991, and the date of the ruling was May 15th, 1992 (Southern African Legal Information Institute (SAFLII, 1992).

It is a criminal offense, in accordance with Section 4(1)(b) of the Protection of Information Act 84 of 1982, to divulge to an unauthorised person particular kind of documents or information that pertain to topics pertaining to the military and that are of a secret or confidential character (South Africa, 2013). And the Riotous Assemblies Act 17 of 1956 makes it an offense for any person to plot with any other person to facilitate or procure the commission of, or to commit, an offense that is either statutory or common law in nature. This provision may be found in Section 18(2) of the act. On February 4, 1988, an ordinary court martial found the three respondents guilty of violating section 4(1)(b) of Act 84 of 1982 when read in conjunction with section 18(2) of Act 17 of 1956. Each respondent was given a sentence of 18 months in detention as a result of their convictions. At the time, the respondents were performing their national service in the Citizen Force in accordance with the Defence Act 44 of 1957 ("the Act"). Additionally, the third respondent, who at the time held the rank of corporal, was demoted to the lowest position possible, which is the third rank.

5.4 MINIMUM INFORMATION SECURITY STANDARD (MISS) 1998

A Cabinet paper on the topic of national information security policy was authorised in 1998 and was referred to as the MISS document. The duties and obligations of the individuals in charge of the organisation are laid forth in Chapter 3 of the text. The classification and declassification system are discussed in Chapter 4, which is relevant to the topic of information security. The MISS (1998) guidelines detail the requirements that ought to be satisfied for applicants to be vetted before their appointment in a sensitive position or in an environment involving crime intelligence (CI). These requirements should be met before an applicant can be considered for a position in either of these settings. Current military personnel, individuals seeking promotions in sensitive situations, and contractors are all required to comply with these regulations (South Africa, 1998: 1). As a consequence of this, it is absolutely necessary for people who work for the government and anyone who want to conduct business with the government to become familiar with the requirements that are specified in the document (Nkuna, 2020: 23).

The topic of personnel security is discussed in Chapter 5 of the MISS paper (1988), which also establishes guidelines for vetting investigations across all government departments (Nkwana, 2017:26). The vetting criteria, the vetting of people who have lived and worked overseas for an extended period of time, the vetting of contractors who intend to conduct business with the State, the procedure for requesting a vetting investigation, the transferability of a security clearance, the responsibilities of the employees who are traveling, and the period of time that a security clearance is valid all apply to the government departments. According to Mahlatsi (2019: 24), the security clearance acts as a guide for the department in terms of the quantity of information that an employee is permitted to access; nonetheless, the need-to-know principle governs this aspect of the situation. In addition to this, it details the processes that should be carried out in order to ensure that the screening of the suitability of security professionals and the validity of security clearances are carried out correctly (South Africa, 1998).

5.5 PROTECTION OF PERSONAL INFORMATION (POPI) ACT

The POPI Act was developed in response to a detailed investigation of worldwide privacy laws conducted by the South African Law Reform Commission (SALRC), which based the act's principles primarily on those implemented by the Organisation for Economic Cooperation and Development (OECD) and the European Union (EU) (South Africa, 2013: 11). SALRC advised that, similar to the strategy taken by the EU, a body be formed to enforce, monitor, and promote conformity to the implemented data protection laws. As a result, the POPI Act requires the government to designate an Information Regulator to guarantee the application and promotion of the rights it protects (South Africa, 2013: 17).

Personal data and information are defined under the POPI Act as any information that allows a user of the information to identify the data subject, who might be a natural or legal person (South Africa, 2013:14). It covers race, marital status, health, gender, sex, pregnancy, ethnic origin, religion, disability, belief, and so on (South Africa, 2013:14), as well as any identifying number or symbol, such as an e-mail address, physical address, phone number, or online identity. According to Greenleaf (2013:236), the legal definition of personal data limits the applicability of data privacy legislation in two ways. Firstly, they do not include data that does not identify a person yet enables for personalised contact with that individual. Examples include the use of software to enable behavioural marketing, in which firms utilise software to create personal profiles that do not include names or internet identifiers but allow for the collection of a considerable quantity of information about individuals (Schwartz & Solove, 2011:1818). "Online identifiers" are included in the definition of "personal information" under Section 1 of the POPI Act.

The second limitation is premised on the exclusion of data kept in a non-transitory form, such as some types of closed-circuit television (CCTV) recordings (Greenleaf, 2013: 236). The ICO publishes a CCTV code of practise (ICO, 2008), which contains guidelines on how and where recorded material should be stored responsibly. The POPI Act does not directly address this matter (South Africa, 2013:14), but the future Information Regulator will be able to advise South African firms on the best business practises to follow when dealing with this sort of content.

The POPI Act has been used in various court decisions, such as in the case of the Black Sash Trust versus Minister of Social Development (Business Insider SA, 2020: 1). This decision principally concerns SASSA's capacity to pay grant recipients across the country in a legal way. SASSA previously outsourced the monthly social grant payments procedure to Cash Paymaster Services (CPS) as part of a prior arrangement In the public interest, Black Sash petitioned the Constitutional Court, asking the Court to declare that any contract between SASSA and CPS should specify that the personal information of grant recipients becomes SASSA's property.

The Regulator objected to Black Sash's proposal, claiming that there was no legal basis to deprive social grant recipients of ownership of their personal information and vest it in SASSA (Southern African Legal Information Institute, 2018: 1). As a result, the court ruled that recipients of social grants control their personal information. The South African Social Security Agency (SASSA) shall only utilise personal information to conduct monthly social grant payments to its recipients, according to the Court. The Court ruled that the contract between SASSA and the CPS should include protections to protect the personal information of grant beneficiaries.

Another similar case involves My Vote Counts, a non-profit organisation that requested an order to gather information about the private funding of political parties and independent candidates (Southern African Legal Information Institute, 2018: 1). The High Court ruled that PAIA does not apply to political parties, independent candidates, or all private fundraising data. The High Court determined that PAIA's failure to give access to information on private funding violates Article 32, 7(2), and 19 of the Constitution when read together. This instance is consistent with security threat assessment in that political parties are critical political entities that should be monitored on a regular basis to avoid insider and outer dangers to the country.

5.5.1 Google Spain SL, Google Inc. v. Agencia Espaola de Protección de Datos (AEP)

In a case involving Google Spain SL, Google Inc. v. Agencia Espaola de Protección de Datos (AEP) Mario Costeja González (case no C-131/12, 13-5-2014). This decision was handed down in a matter between Google Spain SL, Google Inc. The verdict concerned the collection and use of private information or data by Google, which operates a search engine on the internet. Coincidentally, the ruling was handed down at the same time that South Africa's Protection of Personal Information Act 4 of 2013 (POPI) was being officially enacted into law there (SAFLII, 2014).

5.6 NATIONAL KEY POINTS ACT, 1980 (ACT 102 OF 1980)

The National Key Points Act (NLPA), inherited from the Apartheid regime, was enacted in response to a series of sabotage activities against what was deemed to be important infrastructure, and was intended to impose legal consequence on anybody who 'threatened' a national key point (Hlongwane, 2013:1). Crucially, it provided security managers broad authority to designate any location as a national vital point, putting it under the control of enhanced security and secrecy. According to a survey commissioned by the non-governmental organisation Right2Know (R2K), the number of national key points has expanded by more than 50% in the previous five years, from 118 in 2007 to over 182 in 2021 (R2K, 2017).

This law has been criticised for allowing the state to abuse it. This legislation, according to Hlongwane (2013:1), has been utilised to shield otherwise dubious official behaviour from public scrutiny. Simply put, if a facility was designated as a national vital site, the government could conceal it behind a wall of red tape and classifications. The primary goal of the National Key Points Act 102 of 1980 (SA, 1980) was to assess and identify the risks, threats, and vulnerabilities of national key points in the Republic of South Africa. South Africa positions itself as an investor-friendly destination by considering the importance of key infrastructure such as telecommunications, energy production, and banking, because the infrastructure protection policy helps to de-risk the costs associated with doing business in the country (Oforis, Hindle & Hugo, 1996).

5.6.1 Right2Know Campaign and Others v. Minister of Police and Others

In the matter of Right2Know Campaign and Others v. Minister of Police and Others (2013/32512) [2014] ZAGPJHC 343; [2015] 1 All SA 367 (GJ) on the 3rd of December 2014, indicate that the case was about whether or not the people of South Africa ought to know what places and areas are considered national key points, as contemplated by the National Key Points Act 102 of 1980. The case was about whether or not the people of South Africa ought to (NKP Act). According to subsection 11(3) of the Promotion of Access to Information Act 2 of 2000 (PAIA), a "requester" of information does not need to provide a justification for requesting information that is kept by the state as long as the request is made in line with the formal request processes. In the event that the information is not provided, the denial of the request must be justified using one or more of the grounds outlined in Chapter 4 of the PAIA.

5.7 CRIMINAL PROCEDURE ACT, (ACT 51 OF 1977) AS AMENDED

Criminal procedure begins long before a person who has committed an offense is brought to trial in a court of law (South Africa, 1977: 1). In fact, criminal procedure can be invoked even before an offense has been committed. Certain provisions of the Criminal Procedure Act, in particular, Sections 20 and 25, empower police officers to do certain things to prevent the commission of an offense.

Reading the relevant legislative provisions granting people the authority to conduct searches, seize items, and arrest people, one cannot help but notice the repeated mention of reasonableness. Section 20 states that certain articles may be seized if they are "reasonably believed to be" articles of a particular nature. Section 23 states that those who arrest another and are not peace officers are only authorised to seize articles and not to search for them (South Africa, 1977: 1). This implies that a security officer who is not also a peace officer and who is not authorised to conduct a search by another law may not search an arrestee but may seize an article if it falls within the scope of section 20. The arrestee may, of course, freely consent to such a search, in which case the security officer may carry it out. Section 24 states that a person in charge of or occupying land or premises may conduct searches and seize articles if certain conditions are met. Sections 40-43 authorise certain people to arrest people who are "reasonably suspected" of committing certain crimes.

Security officers who provide services at another location, for example, may only do so if they use the powers granted by the Criminal Procedure Act and may not exceed those limits (South Africa, 1977: 1). Any contract that purports to authorise a security officer to take actions that are illegal under the law, such as shooting anyone who attempts to enter the premises, will be deemed invalid.

Section 49(2) of the Criminal Procedure Act authorises the use of blameless killing to accomplish the arrest of those who are reasonably suspected of committing certain crimes. When interpreted in the context of a security threat assessment, the legislation allows an arresting officer to shoot to kill a suspected criminal who constitutes a threat to the government or any of its departments. In recent years, there has been an upsurge in critical infrastructure theft and vandalism, such as copper wires. Odendal (2021: 1) found that cable theft and vandalism cost the country an estimated R187 billion, with critical institutions like as Telkom, Eskom, the South African Passenger Rail Agency, and Transnet losing R7 billion every year. Given this context, law enforcement officers have used section (49) when dealing with suspected criminals on vital infrastructure.

Legal scholars have questioned the legality of Section 49(2). Burchell (2006:200), for example, argues that this provision has been used to justify killing in a variety of circumstances, adding that it violates the right to life, freedom, and security, as well as protection from cruel, inhuman, or degrading treatment or punishment and the right to a fair trial, which includes the right to be presumed innocent (Botha & Visser, 2012:2).

5.7.1 BK and Others v. Minister of Police and Others

In the case of BK and Others v. Minister of Police and Others (22575/2018) [2019] ZAWCHC 91; 2020 (1) SACR 56 (WCC), the applicants seek an order against The Minister of Police as the first respondent, The Directorate for Priority Crime Investigation as the second respondent, and Mr. Mziyanda Mti as the third respondent, setting aside a search warrant issued by a member of the second respondent and ordering them to return to them all items that Everyone *who responded has a negative opinion about the application. The first argument that the respondents make is that because they arrested the first applicant under the circumstances that they did, they were within their rights under Section 20 and, more importantly, Section 23(1)(a) of the Criminal Procedure Act 51 of 1977 to carry out a search and seizure operation at the applicants' residence. This is the respondents' primary contention. When a person is arrested, some items may be seized at their discretion according to the guidelines outlined in Section 23. In any event, the case against the respondents continues, and the search and seizure operation were only carried out after a search warrant was obtained earlier in the evening of the applicants' arrest. This was done at the applicants' and their attorneys' insistence, and it was the only time it was carried out (SAFLII, 2019).*

5.8 CONTROL OF ACCESS TO PUBLIC PREMISES AND VEHICLE ACT 53 OF 1985

The Control of Access to Public Premises and Vehicles Act 53 of 1985 (CAPPVA) was passed in order to protect certain public buildings and cars, as well as the persons who were present in or around those public buildings and vehicles (South Africa, 1985). According to the CAPPVA, the owner of any public premises or any public vehicle, who also happens to be the head of the department of state, division, office, or other body, which occupies or uses those premises or that vehicle or is in charge thereof, depending on the circumstances, has the authority to direct that those premises or that vehicle may only be entered or entered upon in accordance with the provisions that have been laid down (South Africa, 2009: 6).

In addition, the Act confers upon the owner the authority to take whatever precautions he or she may deem appropriate for the purpose of ensuring the safety of the place or vehicle in question, as well as the people who are present in either of those locations or vehicles, and the contents of either of those locations or vehicles. Without the approval of an authorised officer, no one is allowed to enter any public building or any public vehicle that displays a sign indicating that entrance to that place or vehicle is controlled. This notice should be visible at all times (South Africa, 2009: 6). There are many instances where the law is applied to manage risks to national infrastructure as well as safely of people. For instance, Gautrain, premises and vehicles under the control of its operating company have been declared as premises and vehicles for the purpose of the Control of Access to Public Premises and Vehicles Act (1985). Using this law, Gautrain officials are allowed to reach passengers, ask for proof of payment, proof of identity, use electronic tools to search for dangerous weapons and substances and declare any vehicle, container or bag and display them. All these acts help to prevent crimes such as terrorism, use of dangerous weapons in public and robberies, among other serious crimes which pose a threat to humans and critical infrastructure.

5.9 LABOUR RELATION ACT 66 OF 1995

Under Section 66 of the Labour Relations Act, which was passed in 1995, an employer is allowed to fire an employee for misconduct that is both significant and of such a seriousness that it makes it unbearable to continue the employment relationship (South Africa, 1995). The inappropriate behaviour of the employee will be the root cause, and "the job relationship will deteriorate to an unacceptable state" will be the outcome. In the context of this research, it is possible for an employee to be terminated on the grounds that their acts pose a significant risk to the government agency in question as well as to other institutions and individuals (Duff, 2010: 2).

The Act specifies the reasons on which an employer may dismiss an employee, and those grounds are as follows: the conduct of the employee; the capacity of the employee; and the operational requirements of the employer's business. Inappropriate behaviours are those that involve a breach of good faith. In addition, the Act includes a set of principles that can be used to evaluate whether or not dismissals for misconduct are equitable. This indicates that the employee has the opportunity to seek redress in the event that they believe their dismissal was unjustified. An illustration of this can be found in the case of Fredericks v. Jo Barkett Fashions [2011] JOL 27923 Commission for Conciliation, Mediation, and Arbitration (CCMA), in which the employee was fired after the employer learned that the employee had been making negative remarks about the employer on Facebook. In a case where there was no pre-existing policy governing employee conduct, the court convened to decide whether or not the employee should have been fired. On the basis of this legal loophole, it is essential to analyse whether or not the laws that are now in place are effective in managing risks that are internal to the government and come from its personnel (Duff, 2010: 2).

5.9.1 Sedick and Others v. Krisray

In the cases of Sedick and Others v. Krisray (Pty) Ltd (2011) 8 BALR 879 (CCMA) and Fredericks v. Jo Barkett Fashions [2011] JOL 27923 (CCMA), the Commission for Conciliation, Mediation, and Arbitration (CCMA) ruled that the employees were terminated fairly as a result of derogatory Facebook status updates. Because the employees had not configured their Facebook privacy settings to restrict who could view their updates, anyone, including those they were not "friends" with on the platform, could view their status changes. In accordance with the CCMA's interpretation of Section 70 of Act 70 of 2002, "Regulation of Interception of Communications and Provision of Communication-related Information," employers had the legal authority to read employees' private online posts. (RICA). The panel concluded that the employer had the legal right to see the wall posts made by the employees since those employees had "open" Facebook pages, which did not infringe the employees' right to privacy.

5.10 NATIONAL ARCHIVES ACT, 1996 (ACT 43 OF 1996)

In South Africa, the National Archives and Records Services of South Africa Act (Act No. 43 of 1996, as amended), which became operational in 1997, represents a significant turning point for archives and the archival profession. The Act was first passed in 1996. (Netshakhuma, 2019: 5). It does so by bringing the management and administration of public archives into conformity with the constitution of the nation, which was first implemented in April of 1994. According to Garaba (2012: 33), despite the fact that the Act shares many similarities with earlier archive legislation, there are also a number of significant distinctions between the two pieces of legislation. These are highlighted in the provisions for the management of the National Archives, outreach activities, access to archival holdings, the management of current public records, the collection and management of non-public records, and the establishment of provincial archives services. In addition, there are also provisions for the establishment of provincial archives services (South Africa, 1994). The construction of archives buildings not only fulfils the function of providing a location to store the historical record, but also serves as a tangible representation of the significance of a nation's cultural legacy (). When it comes to the protection of archive materials, the structure serves as the initial line of defence. The facilities that house archives are required to be secure enough to prevent theft, detect and put out fires, and protect documents from damage caused by earthquakes and floods.

5.11 PRIVATE SECURITY INDUSTRY REGULATION ACT 103 OF 1996

Because of a variety of factors, it has become clearer that the existing regulatory system in South Africa requires an examination, as well as changes and transformations (South Africa, 2001). The end of apartheid brought about significant shifts in both the political climate and the physical makeup of the country. Because the existing legislation for the PSI was written before the Constitution of 1996 was enacted for the Republic of South Africa, it was not entirely consistent with all the values and principles outlined in the new Constitution. This was due to the fact that the new Constitution was adopted in 1996. Because of these shifts, there is now a pressing need to ensure that newly enacted laws are in line with those that already exist and are applicable to all facets of the security business (Gumedze, 2008: 110).

The Private Security Business Regulation Act came into effect in 2001 and was the last piece of legislation that was necessary to regulate the private security industry in South Africa. This Act was presented to the President for his signature on January 15th, 2002, and it went into effect two months later February 14th, 2002. This new Act filled in some of the flaws that were found in the previous legislation while also repealing the Security Officers Act, 1987 (also known as Act 92 of 1987) and any later revisions to it. This act passed in 2001 broadened the scope of the legislation by expanding and defining the term "security service providers" to include both private security officers and commercial enterprises. In addition to this, the Act provided for the establishment of a new regulating organisation that would be known as the Private Security Industry Regulatory Authority (PSIRA).

According to Section 3 of the PSIRA Act 56 of 2001, the primary goal of the Authority is to regulate the PSI and to ensure that the practices of security service providers are in accordance with public and national interests in addition to the interests of the private security industry. This objective was stated in the PSIRA Act 56 of 2001. The pursuit of "profit maximization" is the primary motivation for many private security businesses in South Africa, and this can be to the cost of the interests of their customers. A circumstance of this nature gives rise to the requirement for efficient protective regulations (Gumedze, 2008: 11). As Berg and Gabi (2011:3) pointed out, many private security organisations work to take advantage of market opportunities, boost their turnover, and raise the amount of money returned to their shareholders. To ensure that citizens of South Africa have a sense of safety, security, and protection against unscrupulous and exploitative operators, therefore, it is vital to have adequate regulation of the PSI in that country. A further requirement of the regulation is that private security businesses should transform themselves into reliable and reputable organisations that operate within the bounds of the law (Gumedze, 2008: 11).

In South Africa, various government departments have established their own internal security infrastructure (Govender, 2018: 137). The PSIRA has also registered these members of the security staff. Civilian powers were granted to them in accordance with Act 51 of the Criminal Procedure Act in 1977. Some internal security personnel are given the authority to carry out their duties by national legislation that is pertinent to the individual government department where they are working. These officers are employed by specific government departments. They address information on security incidents, threats, and vulnerabilities depending on the business case presented by the government department.

The SAPS receives information concerning criminal incidents for the purpose of conducting investigations (Govender, 2018: 137). The people of South Africa should be given top priority under the Act, and they should be given the ability to act against and prevent crime. In the same manner that a foreign person who has been in the country for fewer than fifteen years is not eligible for a Top Security Clearance (TSC), the government should not permit a foreign national to perform private security services. This is because, on both a micro and a macro level, people in South Africa are loyal to their government.

5.11.1 Union of Refugee Women and Others v Directo

Union of Refugee Women and Others v Director, Private Security Industry Regulatory Authority and Others (CCT 39/06) [2006] ZACC 23; 2007 (4) BCLR 339 (CC); 2007 (4) SA 395 (CC) was a case that was heard on December 12, 2006. This application seeks to establish the rights of refugees to find employment in the private security industry in South Africa. This industry is governed by the Private Security Industry Regulation Act 56 of 2001, sometimes known as the "Security Act." This matter was brought before the Court in the form of an application for leave to appeal against the judgement made by Bosielo J. in the Pretoria High Court. The High Court of South Africa reached the conclusion that section 23(1)(a) does, in fact, provide South African citizens and permanent residents with preferential treatment. However, the court emphasized that this clause cannot be interpreted in isolation. As a consequence of this, it concluded that the provision of section 23(1)(a) was sufficiently mitigated by section 23(6) to be in accordance with the constitution (SAFLII, 2006).

The High Court stated the following in its analysis of the rationale behind section 23(1)(a): "It is understandable, in my opinion, that due to the high level of trust required by private security officers, there should be some strict criteria as to who can qualify for such positions in order to exclude undesirable persons." Although the court expressed sympathy for the plight of refugees, especially given their vulnerable position in society, the High Court held that the public's safety and security, as well as the protection of vulnerable individuals, were more important

5.12 PROMOTION OF ACCESS TO INFORMATION ACT, 2000 (ACT NO 2 OF 2000)

The objective of the Act is stated in both the Preamble and section 9 of the PAIA, and there is some degree of overlap between the two provisions (Khumalo, Bhebhe & Mosweu, 2016: 16). In general, the purpose of the Act is to make it possible for an individual to obtain access to information in order to make it easier for that individual to safeguard and exercise his or her rights, as well as to promote the ideal of openness and accountability in public and private organisations (van Heerden, Govindjee & Holness, 2014: 27). The Act proposes to accomplish this by establishing methods or mechanisms that would enable an individual to acquire access to such information as "quickly, affordably, and effortlessly as practically possible." This access would be made possible by the Act (van Heerden et al., 2014: 27).

According to Khumalo et al. (2016: 17), the right of access to information should be understood as the right to have the systems in place so that one can acquire access to the information that he or she requires. They offer the internet as an example: having the right to access information would not necessarily provide one with the vast amount of material that is available on the world wide web; rather, it would ensure that the public has access to the internet in an appropriate manner (Khumalo et al., 2016: 17). When viewed in this light, the legislation governing freedom of information should be regarded as a tool that one can employ in order to acquire access to information, thereby enforcing the constitutional right to access information.

According to the law, every citizen has the right to protect the country from any potential risk, and as a result, they have the ability to make a request to gain access to information in order to uphold the constitutional obligation to ensure that those serving in public offices do not pose a threat to the country (Khumalo et al., 2016: 16). This right is understood within the context of security threat and risk assessment. It is possible, thanks to the provisions of PAIA, to obtain information not only from private individuals but also from official agencies. However, as a consequence of the provisions of the constitutional requirement, a requester is expected to be able to provide a justification for why the information is sought from a private individual (South African Human Rights Commission, 2016: 2).

Both "over-restrictive" and "under-inclusive" are two of the criticisms that have been levelled at the PAIA (van Heerden et al., 2014: 27). The Act is excessively restrictive due to the fact that, whereas the Constitution guarantees the right to access "any information held by the state," PAIA narrows the scope of this right to include only "a record held by a public body." This is in contrast to the Constitution, which guarantees access to "any information held by the state."

5.13 OCCUPATIONAL HEALTH AND SAFETY ACT, 1993 (ACT 85 OF 1993)

The Occupational Health and Safety Act no. 85 of 1993 includes its own definition, which can be found inside the act itself. The Occupational Health and Safety Act No.85 of 1993 is the most comprehensive piece of legislation in South Africa dealing to occupational health and safety (South Africa, 1993). The Occupational Health and Safety Act no. 85 of 1993 aims to establish the legislation required to ensure that all individuals have the opportunity to maintain their health and safety while working in an environment that is conducive to that goal (Ali, 2021:2).

One of the most essential sections of the Act is number 8, which deals with the responsibilities of employers. If this section is successfully applied, it will ensure that the departments have dealt with and handled the majority of the Act's requirements (Tshoose, 2011: 166). It is the duty of an employer to ensure that their employees are able to perform their jobs in a setting that does not compromise their health or safety in any way. Employers are also encouraged by Section 8 to review work locations, conduct risk assessments, and conduct routine health and safety inspections of their facilities.

In the event that an employee sustains an injury or develops an illness, the employer is required to inform the DoL. In the event that any high-risk risks materialize, such as a chemical leak, the employer is required to notify this information as well (Tshoose, 2011: 166). The DoL will investigate the events or dangers and make certain that all employers and employees have done their utmost to comply with the Occupational Health and Safety Act and to try to stop the occurrence from happening again. In the event that carelessness was present, either the employer or the employee could be held criminally responsible for their actions or lack of actions (Ali, 2021: 3). The Act is connected to the current subject of the study in the sense that dangers to employees can constitute a major risk to the institution as a whole as well as to the nation as a whole.

5.13.1 Joubert v. Buscor Proprietary Limited

Joubert v. Buscor Proprietary Limited (2013/13116) [2016] ZAGPPHC 1024 was heard on the 9th of December 2016, in the Pretoria branch of the South African North Gauteng High Court. In his decision, the then Acting Judge of the High Court, Siwendu AJ, stated that he had relied on pre-existing principles and must revisit section 9 (1) of the act, which states that "Every employer shall conduct his undertaking in such a manner as to ensure, as far as is reasonably practicable, that persons other than those in his employment who may be directly affected by his activities are not thereby exposed to hazards to their health or safety" (own employees). Regulation 5 (1) states that there shall be no failure (SAFLII, 2016).

To arrive at the conclusion that the old common law test for negligence is met, it is necessary to compare and contrast the elements with the principles. Throughout the course of time, these were refined and reformulated on several occasions. Both Ngubane v. South African Transport Services and Kruger v. Coetzee are now pending before the court. This evaluation serves as an objective test that can be applied in both civil and criminal proceedings. A method of assessing responsibility that is based on a breach of a reasonable person's standard of care has developed over the course of case law, and this is the factor that unites all of these cases. The judgment in the matter of Herschel v. Mrupe places an emphasis on the fact that the test is not arbitrary and is instead based on the facts of the particular case. As I have mentioned before, the Occupational Health and Safety Act of 1993 (Act 85 of 1993) imposes a responsibility and a standard of care on an employer, which results in the company being held to a strict liability standard. The criteria for determining whether or not the employer's measures are reasonable are well-established.

5.14 ELECTRONIC COMMUNICATION AND TRANSACTION ACT 2002 (ACT 25 OF 2002)

Security and privacy are major concerns in Internet banking and other Internet-related transactions. To address these issues, the South African government enacted Act No. 25 of 2002 on Electronic Communications and Transactions (ECT) (Dyer & Bowmans, 2021:3). In South Africa, the Act governs all electronic communication transactions. Businesses implement the Act by, for example, establishing a privacy policy statement on their websites that, in compliance with the ECT Act, specifies how the organisation would use any personally identifiable information submitted by the customer (Dyer & Bowmans, 2021: 3).

Banks and other companies implement the ECT Act by posting a privacy policy statement on their website (Kabanda, Brown, Nyamakura & Keshav, 2010: 3). A statement like this one outlines how the site will utilise personally identifiable information received through fields and forms during web-based transactions.

A privacy policy statement is regarded as an essential tool for banks to use in demonstrating their trustworthiness to their clients. As a result, banks should have a privacy policy statement that complies with the ECT Act in order to demonstrate their trustworthiness (Kabanda *et al*., 2010: 4). The Act's primary purpose is to safeguard banks and consumers from the growing hazards of digital fraud. Due to the victimisation of government agencies through digital fraud, the law enacts safeguards to monitor electronic transactions and raise red lights when appropriate.

5.15 STATE INFORMATION TECHNOLOGY AGENCY ACT, 1998 (ACT 88 OF 1998)

According to Section 2 of the State Information Technology Agency Act (SITA), it is a legal entity formed by the Act. The Act is administered by the DPSA, and the Act is the custodian of SITA. Section 21 of the Act establishes a framework for monitoring information systems in government agencies. Section 6 of the Operate further states that "in relation to these services, it should act as the agent of the South African Government" (Department of Water Affairs and Forestry [DWAF], 2021: 1).

It should be mentioned that the purpose of the Act is to centralise the availability and administration of data to the SITA. However, it is worth noting that Section 7 of the Act, which deals with the Agency's powers and activities, does not contain the Agency's ability to dispose, exchange, or disseminate information. The present study's focus is on how SITA, as a trusted government agency, maintains sensitive government information and records in light of risk and threat management methods.

The central aspect of this realisation is that, at this point, SITA's mandate focuses upon information storage and technical progress of information systems for the benefit of participating departments. What is unclear is the decision of disposal, exchange, or sale of information relating to the participating department as it is commonly understood. This is where possible dangers in government information management may be found.

5.15.1 SAAB Grintek Defence v South African Police Service and others

In the case of SAAB Grintek Defence v South African Police Service and others (2016) 3 All SA 669 (SCA), it was decided that the SITA Act does not give SITA the authority to award tenders or conclude contracts on behalf of departments. Instead, the SITA Act requires SITA to facilitate the acquisition of technology services by government departments.

5.15.2 SITA (Pty) Ltd v Premier, Eastern Cape Provincial Gov. and Others

State Information Technology Agency (Pty) Ltd v Premier, Eastern Cape Provincial Government and Others (250/2018) [2018] ZAECBHC 12 was a case that was heard on October 23, 2018. According to the Judgement, the State Information Technology Agency (Pty) Ltd ("SITA") was attempting to get an order reviewing and setting aside a contract for the roll-out of broadband services that was awarded by the Eastern Cape Provincial Government on 11 October 2017 to Liquid Telecommunications South Africa (Pty) Ltd. (SAFLII, 2016).

According to the judgment, it is a matter of common cause that the contract was not awarded to Liquid Telecoms through a competitive bidding system; rather, it was awarded to them through Treasury Regulation 16A6.6, which permits an accounting officer of a department to participate in a contract concluded by another organ of state through a fair, transparent, and competitive bidding process. This regulation was used to award the contract. The only requirement is to receive permission from the appropriate state organ as well as the department providing the service.

5.16 THE PUBLIC SERVICE ACT, 103 OF 1994

Section 3 (4) of the Public Service Act, 103 of 1994, specifies security guidelines to which officials and staff have to adhere. According to Section 17 (2) (h) of the Public Service Act of 1994, an employee may be fired if their continued employment poses a security risk to the state. Section 20 of the Public Service Act of 1994 addresses specific sorts of misbehaviour that, in certain situations, may result in security screening. Some employees are covered by this Act, and it is critical that all members and prospective employees follow this provision of the Public Service Act, 103 of 1994. The involvement of the finance and human resources heads of business in the security committee and implementation of STA, will ensure that there no employees that are earning multiple salaries.

5.16.1 SA Public Servants Association obo Ubogu vs Head of the Department of Health

In the case of SA Public Servants Association obo Ubogu vs Head of the Department of Health, Gauteng and Others, Head of the Department of Health, Gauteng, and Another vs Public Servants Association obo Ubogu (CCT6/17, CCT14/17), [2017] ZACC 45; 2018 (2) BCLR 184 (CC); (2018) 39 ILJ 337 (CC); [2018] 2 BLLR 107 (CC); 2018 (2) SA (7 December 2017). The constitutionality of a statutory provision is at issue in this case. That provision permits the state, in its capacity as an employer, to recover monies that were improperly paid to its employees by deducting those sums directly from their salaries or wages, even in the absence of any agreement between the parties or due process. Issues pertaining to self-help, which is an element of the rule of law, procedural fairness, and the idea of set-off in common law are brought to the forefront as a result of this. The primary questions that need to be answered are whether the order of constitutional invalidity issued by the Labour Court falls within the ambit of section 167(5) of the Constitution and therefore needs to be confirmed by this Court, or whether or not it is an interpretative order that does not need to be confirmed. In the event that the ruling is a declaratory order of constitutional invalidity, and it is upheld, what type of remedy is considered appropriate? Should the appeal of the respondents be granted if it turns out that the declaration of invalidity was incorrect (SAFLII, 2017).

The Labour Court ruled that Section 38(2)(b)(i) of the Public Service Act (Act) was unconstitutional, but it used an interpretative remedial mechanism to resolve the flaw in the provision. This section gives the state the authority, as an employer, to recover monies wrongfully paid to its employees directly from their salaries or wages, without the need for due process or agreement.

5.17 THE EMPLOYMENT EQUITY ACT, 55 OF 1998

The Employment Equity Act, 55 of 1998, emphasises that a person may not be unfairly discriminated against in any employment policy or practise, either directly or indirectly. The vetting inquiry should be undertaken in a fair and objective manner. A vetting institution, for example, cannot discriminate against an employee based on their religious beliefs, sexual orientation, or other grounds without following due procedure, as provided in the Labour Relations Act, 66 of 1995.

5.17.1 Harksen v. Lane NO and Others

In the case of Harksen v. Lane NO and Others (CCT9/97) [1997] ZACC 12; 1997 (11) BCLR 1489; 1998 (1) SA 300, which was heard by the Constitutional Court on October 7, 1997, and which is applicable under section 9(3) of the Constitution, but which states that there is no Court in Minister of Finance and Another v. Van Heerden, the Constitutional Court ruled that there is no Court. The primary concern of this inquiry is to determine whether or not the action done may be considered a lawful affirmative action measure in accordance with the parameters outlined in Section 9(2) of the Constitution. If this is the case, then any discrimination that would take place would not be unjust (SAFLII, 1997).

5.18. INTELLIGENCE SERVICE OVERSIGHT ACT, 1994 (ACT 40 OF 1994)

Intelligence oversight is also concerned with the questions that intelligence agencies ask and pursue. This is to examine if the intelligence community is carrying out its mandate and responding to policymakers' demands (South Africa, 1994). It is also to determine whether the intelligence community is aggressive and thorough in its analysis, as well as whether it has the necessary operational capabilities (gathering and covert operations) and resources. Policymakers cannot rely just on intelligence personnel to provide answers to the issues they raise.

Section 3 of the Intelligence Services Oversight Act of 1994 established the JSCI as a parliamentary oversight mechanism and outlines its legislative mandate as follows:

- To collect audit and other reports from the Auditor-General and to review financial figures provided by the intelligence services;
- To acquire from the Evaluation Committee a report on the evaluation that was carried out on the intelligence services, along with any comments or recommendations that may accompany the report;
- To acquire from the designated Judge a report pertaining to the functions conducted in accordance with the Regulation of Interception of Communications and Provisions of Communication-Related Information Act of 2002, including statistics of interception requests made by the intelligence services; and
- To review the report and certificates that were given to it by the IGI and to provide recommendations based on those reviews.

According to NA Rule 137(2) and NCOP Rule 102(2), "each committee does its business on behalf of the House and should thus report to the House on the topic presented to it for consideration." "The South African JSCI is comparable in function to the Canadian Security Intelligence Review Committee (CSIRC)," Hannah et al (2005:23) write. Furthermore, Section 4(1) of the Intelligence Services Oversight Act of 1994 "authorises the JSCI to have access to intelligence, information, and documents in the Intelligence Service's custody or control." Parliament uses these mechanisms as crucial oversight tools to check the operation of the intelligence agencies. According to Section 5(1) of the Oversight Act, "the JSCI should exercise its activities in a way compatible with the safeguarding of national security, therefore the necessity to adequately oversee the screening of committee members."

Dlomo (2004), on the other hand, stated that owing to resource restrictions and strong demand for vetting, it is not always possible to vet all JSCI members. In addition, Section 3(a)(ii) of the Intelligence Services Oversight Act of 1994 "authorises the JSCI to receive the Review Committee's report on the evaluation of the secret services accounts and spending of the SSA." According to the JSCI's Annual Report (2009/10), "the committee has a Memorandum of Understanding with the Auditor-General, who also trains its members." Dlomo's (2004:75) discovery that "there is a significant degree of absenteeism in the attendance of JSCI sessions by committee members" was cause for alarm.

This is mostly owing to the committee's allocation of senior party members, who frequently have other party commitments to fulfil. Gusy believes that "the parliamentary oversight institutions are not only blind guardians, but they are guardians without a sword" (Dietrich, 2015: 135). This is mostly due to a dearth of intelligence-related competence among members of parliament.

5.18.1 Masetlha v. President of the Republic of South Africa and Others

In the matter of Masetlha v. President of the Republic of South Africa and Others (Independent (CCT38/07) [2008] ZACC 6; 2008 (5) SA 31 (CC); 2008 (8) BCLR 771 (CC), Masetlha v. Minister for Intelligence Services (Freedom of Expression Institute as Amicus Curiae), Independent Newspapers (Pty) Ltd. v. Minister for Intelligence Services (Freedom of Expression Institute as Amicus Cur (22 May 2008). The document that has been requested is associated with the case known as Masetlha v. President of the Republic of South Africa (the underlying matter), which was brought before this Court and decided upon by it. It is possible that a rundown of what happened in the Masetlha case might be helpful. Until the President suspended him in 2006 and eventually fired him from his position as Director-General of the National Intelligence Agency, Mr. Masetlha served in that capacity (SAFLII, 2008).

The stipulations of Section 209(1) of the Constitution, as well as the terms of the Intelligence Services Act 65 of 2002 and the Intelligence Services Oversight Act 40 of 1994, were followed in order to establish the National Intelligence Agency (NIA). Mr. Masetlha was required to submit two applications to the High Court in Pretoria (the High Court). In the first application, he contested his suspension, arguing that it had been carried out in an improper and illegal manner. In the second case, he sought to review and overturn the decision of the President to terminate his appointment. In November 2006, the applications for suspension and termination were merged into a single case before Du Plessis J, who heard both cases simultaneously. Both applications ended up being rejected.

5.19 FIREARM-ARM CONTROL ACT, 2002 (ACT 60 OF 2003) AND REGULATIONS.

South Africa also has a history of granting guns licences without "due scrutiny." The Arms and Ammunition Act, which was more of a choose, pay, and get a licence system, governed firearms. In 1996, the Minister of Safety and Security, Sydney Mufamadi, created a special task team to study firearms law, CFCR administration, and the policy on licence issuance. As a result of the task team's recommendations, the Minister of Safety and Security formed a committee to draft new firearms Act to better regulate firearms. The FCA was then designed to replace the out-of-date and heavily amended Arms and Ammunition Act of 1969 (Matzopoulos, Simonetti, Prinsloo, Neethling, Groenewald, Dempers, Martin, Rowhani-Rahbar, Myers, & Thompson, 2018: 197).

South Africa's parliament approved the Firearms Control Act (FCA) in 2000 to better equip police and courts to deal with firearm-related violence. The FCA was introduced in stages and was completely operational on July 1, 2004. The FCA's mission includes, among other things, the following:

- improve the constitutionally guaranteed rights to life and physical integrity;
- to prevent criminality involving the use of weapons, restrict the growth of unlawfully owned firearms by providing for the removal of firearms from society and enhancing control over legally acquired firearms;
- allow the state to remove unlawfully possessed weapons from society, control the supply, possession, safe storage, transfer, and use of firearms, and detect and punish careless or criminal firearm usage;
- create a comprehensive and effective firearms control and management system; and
- ensuring effective monitoring and enforcement of gun control legislation

The FCA added an extra control or monitoring step to weapon applicants in the form of a competence certificate. The competence certificate is required for all persons who handle weapons by virtue of ownership or in the execution of their tasks, such as security officers and those working for gun shops, even if they do not own firearms. This monitoring component was missing in the Arms and Ammunition Act of 1969, which resulted in several irresponsible firearm occurrences at organisations such as security firms (Matzopoulos et al., 2018: 197).

The parts of the FCA that follow outline the prerequisites for obtaining a competence certificate: Section 6 (2) of the FCA states that no licence may be provided to someone who does not have the requisite competency certificate. Section 9 (2) of the FCA states that a competence certificate may only be provided to a person who is 21 years of age or older, in good mental health, and not prone to violence.

5.19.1 Justice Alliance of SA and Another v. National Min. of Safety and Security and Others

It was stated in the case of Justice Alliance of SA and Another v. National Minister of Safety and Security and Others (646/2011) [2012] ZASCA 190 (30 November 2012) that "The Firearms Control Act 60 of 2000 (the new Act), which came into force on 1 July 2004, repealed and replaced the Arms and Ammunitions Act 75 0f 1969." This was stated in the case (the old Act). It governs the possession of weapons in the same way as its predecessor did. In doing so, it recognizes, as stated in its preamble, the store that our Constitution places on the right of every person to life and security, as well as its logical corollary that the increased availability of firearms and the abuse of firearms has contributed significantly to the high levels of crime in our society. In addition, it recognizes that the right of every person to life and security is a right that is guaranteed by our Constitution. The new Act's goals are to "avoid the proliferation of unlawfully possessed firearms and to improve the control of firearms that are legally possessed"(SAFLII, 2012).

It was also decided that "the new Act limits the number of licenses that may be issued to any person in respect of specific types of firearms (sections 13-15) and prohibits the issuance of a license to any person who does not possess a relevant competency certificate (section 6(2))". During those five years, licensees could apply to have their licenses renewed in accordance with the new Act. During those five years, licensees could apply to have their licenses renewed in accordance with the new Act Following the submission of such an application, the license would remain active up until the point at which the application was either accepted or rejected. If an application for the renewal of a license was turned down or if the license was in some other way revoked, the firearm had to be disposed of within sixty days.

5.20 NON-PROLIFERATION OF WEAPONS OF MASS DESTRUCTION ACT, 1993 (ACT NO. 87 OF 1993)

South Africa has always been an outspoken critic of the continued production of weapons of mass destruction, which it views as a threat to international stability and peace. The Non-Proliferation of Weapons of Mass Destruction Act of 1993 is a major piece of legislation that serves as the basis for this. The Non-Proliferation Council was founded by the Act and is funded and supported by the DTI (South Africa, 1993).

The Act provides rules for the registration of commodities, the listing of regulated products, restrictions, the maintenance of confidentiality, annual reporting, offenses and penalties, treaties, conventions, and regimes. The definition of what constitutes a 'controlled good' differs from nation to nation, with each country's legislation being responsible for deciding whether products fall into this category. Parliament gets briefed on the status of the yearly report on an annual basis. The Minister of Trade and Industry is responsible for drafting both official government notices and regulations. In 2010, new laws were passed that imposed restrictions on the registration of chemical products and commodities.

Representatives from the Department of International Relations and Cooperation (DIRCO), the Department of Defence (DoD), the South African Nuclear Energy Corporation (SANEC), the Department of Trade and Industry (DTI), representatives from various industries, the Department of Energy (DEA), and the State Security Agency (SSA) are all present on the Council (Van Wyk, 2021: 14). A Chairperson, a Vice-Chairperson, and a Secretariat composed of members from these regions work together to run the Council.

5.21 PROTECTION OF CONSTITUTION DEMOCRACY AGAINST TERRORISM AND RELATED ACTIVITIES ACT, 2004 (ACT 33 OF 2004)

After receiving a request from the Minister of Safety and Security in 1999, the SAPS carried out research on terrorism and internal security. Based on the findings of this research, the SAPS drafted an Anti-Terrorism Bill, which was then presented to the project committee on security legislation of the South African Law Commission (SALC). This was done in response to an increase in violent crime in the Western Cape (Henning, 2014: 53). It was immediately followed by the first full drawing of the Anti-Terrorism Bill, which was offered for public assessment by the SALC in October 2000. This draught was used as the foundation for Discussion Paper 92, Project 105, which was published in June 2000.

Following the September 11, 2001 terrorist attacks in New York City, the United Nations Security Council (UNSC) passed Resolution 1373, which mandated that all UN member states implement anti-terrorism measures. It was determined that the laws that were already in place in South Africa did not meet all the international requirements relating to the prevention and combating of terrorist and related activities.

In May 20, 2005, former President Thabo Mbeki signed into law the Protection of Constitutional Democracy Against Terrorism and Related Activities Act, 2004, which had previously been introduced in 2004. Act No. 33 of the Year 2004 The Act brings the United Nations Conventions and Protocols Against Terrorism (UNCPAT) and the Convention of the African Union on the Prevention and Combating of Terrorism

(CAUPCT) into full compliance with the Republic of South Africa (Thomashausen, 2007: 22). It provides a wide crime of terrorism as well as offences relating to terrorist activities such as recruiting, help in performing terrorist attacks, and facilitation of terrorist acts. In addition to this, it allows for the specific crimes that are mandated to be criminalised by relevant international instruments to be legislated by individual states. These crimes include terrorist bombings, the financing of terrorism, the hijacking of aircraft, fixed platforms, and ships, the taking of hostages, and crimes that involve protected persons, including diplomatic personnel. As a result, the Act permits the Republic's law enforcement authorities to cope effectively with both foreign and local terrorist operations (Simelane, 2007).

The Act also includes provisions for investigative powers that are comparable to those used in the fight against organised crime, as well as powers of cordoning off, search and seizure, and the surrender of suspects to other States with jurisdiction in circumstances in which a person is not tried inside the Republic. The political exemption for terrorist offenses in terms of extradition is removed as a result of this change. The Act makes it illegal to spread hoaxes such as the ones involving anthrax, which were prevalent all over the world, including South Africa, in the years following the terrorist attacks on the United States of America that took place on September 11, 2001 (Azhar, 2010: 510). According to the Act, an offense includes making a threat, attempting to commit an infraction, conspiring to do so, or inciting another individual to commit an infraction.

The present anti-terrorism policy in South Africa has been operationalized in the form of an anti-terrorism operational model. This model is built on coordination and collaboration between the following entities: intelligence, operations, investigations, protection, and communication. This is achieved through the efforts of the SAPS, the SANDF, the NISS, and any other government institution that is required to be engaged. The mission of gathering intelligence on a strategic, coordinated, and tactical level falls under the purview of the intelligence community. Operations guided by intelligence are carried out with the goals of stabilising a focal region, engaging in tactical intervention in the management of urban terrorism and crowds, and achieving successful control of high-risk activities. Investigations are conducted with the express purpose of achieving fruitful prosecutions as the ultimate outcome (Azhar, 2010: 510).

5.21.1 S v. Okah (CCT) 315/16; CCT

In the issue of S v. Okah (CCT 315/16; CCT 193/17) [2018] ZACC 3; 2018 (4) BCLR 456 (CC); 2018 (1) SACR 492 (CC), on February 23, 2018. [2018] ZACC 3; 2018 (4) BCLR 456 (CC); 2018 (1) SACR 492 (CC). Under the Protection of Constitutional Democracy against Terrorist and Related Activities Act, Mr. Henry Emomotimi Okah, who is a citizen of Nigeria and a permanent resident of South Africa, was charged with 13 charges related to terrorism. Each count carries a maximum sentence of 10 years in prison. Six charges were brought about as a result of two car bombs that went off in quick succession in Warri, Nigeria, on March 15, 2010. Six months later, on October 1, 2010, in Abuja, Nigeria, there was another double car bombing. These six new counts are tied to that event. The explosions in Warri resulted in the death of one person, and the attacks in Abuja resulted in the death of at least eight individuals. Both attacks caused a significant number of casualties and property loss (SAFLII, 2018).

The State was able to prove at the High Court of South Africa, Gauteng Local Division in Johannesburg that Mr. Okah was the mastermind of both bombings and the financier of both of them. The High Court found him guilty on all thirteen charges against him. However, because he was in South Africa when he planned and carried out the bombings in Abuja and was in Nigeria at the time of the bombings in Warri, the Supreme Court of Appeal partially overruled the High Court and acquitted Mr. Okah on four of the Warri charges on the grounds that the Act established only limited jurisdiction over acts that were committed outside of South Africa. This was the basis for their decision. The end result of this was that the sentence of 24 years of imprisonment that the High Court had imposed was reduced to a sentence of 20 years by the Supreme Court of Appeal.

5.22 PUBLIC FINANCE MANAGEMENT ACT, 1999 (ACT 1 OF 1999) AND TREASURY REGULATIONS

One of the most significant pieces of legislation that the democratically elected government of South Africa has passed into law is the Public Finance Management Act (PFMA), 1999 (Act No.1 of 1999, as amended by Act 29 of 1999). It is reasonable to anticipate that a modern Security Manager will have a comprehensive comprehension of the PFMA. This Act encourages the aims of effective financial management in order to maximise the delivery of services by making the most efficient use of the resources that are available (Moagi, 2009: 16). According to Nkoana and Bokoda (2009), the PFMA was first put into effect in April of the year 2000 and was subjected to a series of adjustments reflecting major policy and legislative developments up until the end of the year 2010.

The Exchequer Act (No. 66 of 1975), which had previously been responsible for controlling public financial management in South Africa, was made null and void by the PFMA, which is the most significant law that should be followed in order to direct and beautify the halls of public institutions, as stated by Du Toit et al. (2002: 124). Every accounting officer should first and foremost consult this Act as their primary source of reference. All public authorities should be aware with the Public Finance Management Act in order to guarantee that their acts are within the Act's legislative boundaries. The first democratic administration in South Africa was responsible for passing the PFMA, which was adopted in 1999 as Act No. 1 of 1999 and was later amended by Act No. 29 of 1999.

The Act lends support to the objective of solid financial management, which seeks to maximise service delivery by making the most of the limited resources available to the state in the most effective and efficient way possible. The primary purposes of the Act are to modernize the system of financial management used by the public sector, to give public-sector managers more authority to manage while at the same time increasing their level of accountability, to guarantee that timely access to quality information is always available, and to eliminate waste and corruption in the use of public resources (Moagi, 2009: 1).

The management of public money is carried out in line with a set of principles that have been unanimously adopted as the standard operating procedure across all government departments. These principles are outlined in important documents such as the King Committee's Report on Corporate Governance and the Constitution of the Republic of South Africa, which was passed in 1996. These documents were instrumental in laying the groundwork for the passage of the PFMA. Compliance with the PFMA in public institutions would contribute to good corporate governance standards, as stated in the King Report, which was published in November 1994 and modified in March 2002. (Maude, 2007: 306).

In order to ensure the delivery of high-quality services, it is imperative that all authorities within the departments adhere to the PFMA. They are required to follow the appropriate processes in order to acquire cash for their departments so that they can carry out the purpose for which they were established. Managers who have a solid grasp of the steps involved in making financial decisions are in a stronger position to handle any financial issues that may arise, and as a consequence, have a greater chance of securing the resources necessary to accomplish whatever goals they have set for themselves (Gitman, 2003:8-9).

According to Moagi (2009: 20), public managers are held accountable and responsible for their operations, and they are obligated to make use of government assets in order to provide goods and services to the general public (people). Similar to how money in its monetary form is handled and accounted for, any asset that falls under the purview of public financial management should be safeguarded, put to use in a manner that is both economically and operationally sound, and should also be adequately documented and audited. The PFMA lays a stronger emphasis, as stated by Abedian (2004:18), on accountability for results (outputs and outcomes). The purpose of the PFMA, in its broadest sense, is to improve the effectiveness of government spending operations, an objective that is sometimes referred to as the value-for-money concept.

Compliance with the PFMA has proven to be highly challenging for the majority of departments (Maude, 2007: 309). Compliance with the PFMA is challenging, since it considers both underspending and overspending to be instances of financial misconduct. However, due to the fact that government agencies have not utilised these monies to their full potential, a sizeable amount of money is sent back to the National Treasury. The provision of services is negatively impacted as a result of this situation. Kanyane (2004: 47) claims that the majority of government institutions go over their allotted budgets each and every fiscal year because each ministry spends more than it is allowed to. Despite this, the directors-general are still unable to satisfactorily explain this in detail before the Parliamentary Committee on Public Accounts. Compliance continues to be a challenge on both the national and provincial levels, despite the fact that the PFMA places an emphasis on economical, effective, and efficient financial management. It has been established that a number of government agencies are lacking in performance efficiency, which has negatively impacted their attempts to supply services to the public. These departments are working hard to comply with the PFMA.

According to Maude (2007: 310), line managers and cost centre managers in government departments often come from a variety of backgrounds and have a variety of educational degrees in non-financial sectors. Interpreting and carrying out various financial procedures can be challenging for these managers. The majority of managers have no formal training in financial management. Van Wyk's (2004: 414) investigation discovered the following elements, among others:

- a lack of personnel that is experienced, knowledgeable, competent, and qualified;
- accounting and information systems that are not up to date;

- a lack of comprehension on the Public Financial Management Act, which was passed as Act No. 1 of 1999; and
- inadequate control mechanisms, lack of understanding of accrual accounting, and generally recognised accounting principles. Financial management is the transition from financial control and administration to financial management • Financial management is the transition from financial control and administration to financial management (GRAP).

According to Moagi (2009: 20), Accounting Officers bear enormous obligations under the Public Financial Management Act 1 of 1999 (as modified). The Act delegates four key responsibilities: operating basic financial management systems, including internal controls, in departments and any entities they control; ensuring that government institutions do not overspend their budgets; reporting on a monthly and annual basis, including the submission of annual financial statements two months after the end of a fiscal year; and publishing annual reports in a prescribed format, which introduces performance reporting.

5.23 PROTECTED DISCLOSURES ACT, 2000 (ACT 26 OF 2000)

In a recent report, Transparency International (2010:4) emphasized how important it is to shield employees who blow the whistle from any kind of internal reprisal. Gibbs (2020: 592) asserts that "South Africa has a robust regulatory framework that encompasses several areas of whistleblowing," and that this is seen as an essential approach in the fight against corruption. The South African Constitution Act of 1996 provides additional protection for people who blow the whistle. In light of this objective, Callard and Dehn (2004: 149) pointed out that the South African Constitution (1996) was written with the intention of "creating the foundations for a democratic state in which administration is centred on the will of the people and every individual is equally granted legal protection”.

Alshoubaki and Harris (2022: 4) brought attention to the fact that whistle-blowers are considered to be a vital component of corporate governance, which ultimately results in greater monitoring and control of improper managerial behaviour. It is now generally agreed that insider information from whistle-blowers are the most common and normal means of finding fraud and other forms of misconduct. Act 26 of 2000, often known as the Whistle-Act, blower's is another name for the Protected Disclosures Act, which was passed in 2000. In order to "protect workers from reprisal that might occur when they provide information regarding suspected misbehaviour," the Protected Disclosures Act was enacted. In addition to this, it was put into place to assist in the creation of a secure working environment in which employees are allowed to communicate information in a responsible manner, so supporting good governance and openness. As part of their efforts to combat corruption, whistle-blowers have the ability to utilise the legislative process.

The framework of whistleblowing law in South Africa was formed by the Constitution of South Africa (1996), the Companies Act of 2008 (Act 71 of 2008), and the Labour Relations Act of 1996. The Protected Disclosures Act (PAD) was passed in 2000 and is a part of this structure (Act 66 of 1995). (Botha & Heerden, 2014: 339). According to the preamble, the objective of the Protected Disclosures Act (2000) is "to aid establish a culture that will allow the reporting of unlawful action that persons notice in their departments." The Whistle-blower Protection Act of 2000 acknowledges the possibility that those who blow the whistle could suffer adverse consequences. As a result, in order to combat corruption, the Protected Disclosures Act (2000) safeguards whistle-blowers from any occupational ramifications, allowing them to expose any misbehaviour without fear of retaliation. This was done in an effort to combat corruption.

The Protected Disclosures Act of 2000 protects employees from the following negative consequences:

- Dismissal, suspension, demotion, intimidation, or harassment;
- Being exposed to disciplinary action;
- Being transferred against his/her will;
- Refusal of a transfer or promotion;
- Refusal of a term or condition of employment or retirement that has been changed or is being maintained changed to his/her detriment;
- Refusal of a reference or receiving an adverse reference;
- Denial of appointment to any employment, profession, or office;
- Threats of any of the aforementioned actions; and being adversely affected in any other way in relation to his/her employment, profession, or office, including employment opportunities and job security" (Republic of South Africa, 2000).

Essentially, the Protected Disclosures Act (2000) establishes a clear and simple framework to encourage responsible whistleblowing by assuring employees that remaining silent is not the only safe option; providing strong protection for employees who raise concerns internally; reinforcing and protecting the right to report concerns to public protection agencies; and, finally, protecting more general disclosures provided that there is a valid reason for going wider and that the parity is met (Republic of South Africa, 2000).

Individuals who have been victimised in violation of the Act, whether or not they have been dismissed, can submit a matter to the CCMA, and then to the Labour Court. Employees who are fired for making a protected disclosure may seek payment, up to a maximum of two years' salary, or reinstatement. Employees who are not fired but are harmed in any manner as a result of making a protected disclosure may seek repayment or seek any other suitable direction from the court (Promoting Whistleblowing Act) (No. 26 of 2000).

5.23.1 Symmington v. South African Revenue Services

In the case of Symmington v. South African Revenue Services (60723/2017) [2017] ZAGPPHC 1181. The hearing was brought to my attention on September 15th, 2017, and the disciplinary investigation was scheduled to take place on September 18th and 19th. Nevertheless, the Respondent made it clear during the hearing that it would not proceed with any hearing before I had rendered my judgment. According to the allegations made by the Applicant in the Founding Affidavit, the Applicant made a number of disclosures that meet the criteria for "protected disclosures" as specified in sections 1, 5, and 9 of the Protected Disclosures Act. He said that as a direct result of making those disclosures, he was now facing a disciplinary hearing as well as the possibility of being fired from his position with SARS. He further stated that the revelations were in connection with occurrences that took place on October 18th, 2016. In order to provide context for this accusation, he felt it was important to provide a narrative of "the wider circumstances" that led up to the incident that occurred on October 18, 2016 (SAFLII, 2017).

The majority of those events did not involve him directly; rather, he asserted that the events of 18 October 2016 should be understood in the larger context of the problems associated with state capture and the attempts to remove Mr. Pravin Gordhan from his position as a former Minister of Finance. After that, he began to detail the sequence of events that led to the dismissal of Minister Nene and Minister Gordhan from their respective positions in the government. In that particular setting, his contribution consisted of the drafting, in March 2009, of a memorandum in which he expressed an opinion that the proposed retirement of Mr. Ivan Pillay, a former Deputy Commissioner of SARS, was lawful and in compliance with applicable laws and regulations. In that document, he also expressed an opinion that the proposed retirement.

5.24. GOVERNMENT IMMOVABLE ASSET MANAGEMENT ACT. 2007(ACT NO 19 OF 2007)

GIAMA was established to ensure and achieve coordination between immovable asset usage and service delivery objectives by providing uniformity in the management of immovable assets held or used by a national or provincial government. It also includes rules and minimum acceptable criteria for the administration of public immovable assets (Phathela & Cloete, 2017: 3). GIAMA seeks to improve service delivery by assuring accountability and efficiency throughout the property lifespan, while also conserving the environment and cultural and historic assets (Government Immovable Asset Management Act, No. 19 of 2007, 2007: Chap 1).

GIAMA emphasises the need of each organ of state developing an immovable asset management plan as part of the government's strategic planning and budgeting procedures. The immovable asset management plan should include all assets that a state organ utilises or intends to use. Custodians has to also collaborate with user departments to develop asset management plans that involve effective communication, service level agreements, performance standards, and cost management (Phathela & Cloete, 2017: 3).

5.25 WHITE PAPER ON INTELLIGENCE (1995)

The White Paper on Intelligence (1994) provided some clarity on how the new intelligence regime would be restructured in the aftermath of apartheid. It also stated that the previous minority government's intelligence dispensation's national security focus was flawed because it represented an undemocratic society (South Africa, 1994). Paper 6 also included provisions for a "new national security philosophy" and reflected theoretical foundations for what the word "national security" should mean.

The conventional, almost entirely military strategic vision of national security was seen too limited and insufficient, and a more comprehensive view of national security, one that should represent an approach that includes risks to political, economic, and environmental aspects, was studied. Aspects such as long-term economic development, social justice, and a collaborative approach to conflict resolution were proposed (South Africa, 1994).

The White Paper on Defence (1996) expressed similar ideas, describing national security as a broader all-encompassing notion that concentrated intently on individual security and no longer on one security controlled by military and police measures. These articles established the underlying concepts that govern national security as outlined in the South African Constitution.

These guiding principles should be read against the backdrop of the Freedom Charter (1955), which strives to remedy historical injustices and is enshrined in the Preamble, Founding Provisions, and Bill of Rights of the Republic of South Africa's Constitution (1996). These concepts pervade the South African Constitution and may be found in the majority of its chapters. With these foundational papers and legal framework in place, a solid foundation for a new intelligence regime in South Africa was built. The intelligence environment appeared to be working successfully within its mandate and in accordance with the Constitution until 2005, when it was uncovered that some wrongdoing happened beyond the scope of the intelligence apparatus, which was subsequently to be disclosed as Project Avani (Nathan, 2009: 26; Cepik & Ambros, 2014: 542).

5.26 CANADA THREAT ASSESSMENT

5.26.1 The National Security Act, 2017 accomplishes three important objectives:

According to Public Safety Canada (2019), the National Security Act, 2017 (hence referred to simply as the National Security Act) was granted royal assent on June 21, 2019. This bill brings Canada's security and intelligence legislation up to date and strengthens them by giving Canadian agencies the clear constitutional and legal framework they need to execute their duties effectively while preserving the rights and freedoms of Canadian citizens. The Act accomplishes three important goals:

5.26.1.1 Increasing Accountability and Transparency

The outcomes of the public consultation on national security revealed that the general public has a need for improved accountability and transparency on matters pertaining to national security. As will become clear in the next paragraphs, the National Security Act of 2017 responds to this requirement in a number of different ways.

5.26.1.2 Fulfilling Commitments to Address Former C-51

During the course of the consultation, the people of Canada made it quite clear that they anticipate having their rights and freedoms safeguarded in addition to their safety. The steps that are mentioned in this section indicate how the old Bill C-51's concerns are addressed by the National Security Act of 2017, which is currently in effect.

5.26.1.3 Strengthening Security and Safeguarding Rights

The legislative landscape and the political context in which it functions need to adapt in tandem with the ever-changing threat environment. The provisions that are mentioned in this part indicate how the National Security Act of 2017 strengthens Canada's capability to respond to new threats while simultaneously preserving the rights and freedoms of Canadian citizens.

5.26.2 The Security of Canada Information Sharing Act (SCISA)

National Security Green Paper (2016: 12) reports that the Security of Canada Information Sharing Act (SCISA) was created by Bill C-51 (the Anti-terrorism Act, 2015), which established additional authority for national security information sharing. It gives all federal government institutions new, explicit authority to disclose information related to "activity that undermines Canada's security" to certain designated federal institutions with national security responsibilities. This excludes activities such as protest, advocacy, dissent, and artistic expression. The SCISA prohibits the disclosure of information about these activities.

National Security Green Paper (2016: 11) indicates that for the past 30 years, the Canadian system has worked as follows:

- CSIS gathers information on suspected threats to Canada's and Canadians' security, both at home and abroad,
- CSIS advises other government agencies – such as law enforcement – on the threats, and
- These other agencies act on the information.

National Security Green Paper (2016: 11) further reports that CSIS was given a new mandate to take direct action to reduce threats to Canada's security when Bill C-51 (the Anti-terrorism Act, 2015) was passed. This is referred to as "threat reduction" or "disruption." These threats are defined in the CSIS Act and have not changed in 30 years. To be clear, CSIS does not have the authority to arrest people. However, it now has the authority to take prompt action to mitigate a threat, such as disrupting financial transactions or interfering with terrorist communications.

The CSIS should have reasonable grounds to suspect that an activity is a threat to investigate. CSIS has a higher threshold for threat reduction measures – it should have reasonable grounds to believe that an activity is a threat. All threat reduction measures should be reasonable and proportional to the circumstances, and they have to be subject to explicit constraints. For each threat reduction measure, CSIS should conduct a risk assessment and consult with law enforcement and other agencies, as directed by the Minister of Public Safety and Emergency Preparedness (National Security Green Paper, 2016: 11). Depending on the actions it intends to take, the law requires CSIS to obtain a warrant before proceeding, especially if the measures could jeopardize Canadians' rights as enshrined in the Charter.

5.26.3 Canadian Cyber Security

The National Cyber Danger Assessment (NCTA) forecasted in 2018 that cybercrime will continue to be the most prevalent threat faced by Canadian enterprises of all sizes. This is according to the Canadian Centre for Cyber Security (CCCS) (2020:3). However, other types of cyber threats, such as cyber espionage, have the potential to have a more significant effect. Information can be held for ransom by cyber threat actors, or they can sell it or exploit it to obtain an unfair edge in competitive situations. Attacks using ransomware and targeting industrial processes have become increasingly common over the past few years. These attacks have significant repercussions, including a negative impact on reputation, a reduction in productivity, potential legal repercussions, increased costs for recovery, and damage to infrastructure and operations. They are of the opinion that ransomware attacks aimed against Canada will probably keep focusing on major businesses and the companies that supply essential infrastructure over the course of the next two years.

Shariff and Bisson (2021) concur with CCCS (2020:3) in their assessment that the number, sophistication, and cost of the cybersecurity threats that face Canadian enterprises are continuing to expand. According to a recent article published by Canadian Security, the results of a survey conducted by 2020 with 251 Canadian CIOs, CTOs, and CISOs found that the number of digital attacks had increased over the course of the previous year for all of the survey participants with the exception of one percent. However, 86 percent of the executives claimed that the digital assaults their firms were experiencing had gotten more sophisticated over the course of the same period of time, and all of the respondents said that their company had been the victim of a security breach over that same span of time. During the same time period, Yahoo Finance Canada published an article stating that the average cost of a data breach in Canada had increased by 6.7% since 2019 to reach $6.35 million, making it even more difficult for Canadian organisations to recover from the security incidents that they had suffered.

Information held by Canadian enterprises, such as intellectual property and consumer and client data, is also put at risk by those posing a cyber threat to the country. Theft of this information can have immediate as well as long-term repercussions for the victims' finances, including implications on the victims' worldwide competitiveness and reputational harm. During the COVID-19 pandemic, state-sponsored cyber threat actors targeted Canadian intellectual property related to COVID-19 combat, and we believe that this will continue to support their own domestic public health responses or profit from illegal reproduction by their own firms. In addition, we believe that this will have a negative impact on Canada's international reputation (CCCS, 2020:5).

Cyber threat actors also take advantage of trusted business relationships that exist between Canadian organisations, target both online and in-person payment systems, exploit supply chain vulnerabilities, and take advantage of the privileged access managed service providers have to their customers' networks. These actions may be used to commit fraud against corporations, initiate assaults using ransomware, steal confidential information as well as data pertaining to clients and customers, and so on. A growing range of cyber risks are posed to vital infrastructure providers in Canada, including small and medium-sized enterprises, governments, universities, and other educational institutions. These organisations have control over a wide variety of assets that are of interest to actors that pose a cyber threat. These assets include data about customers, partners, and suppliers; financial information and payment systems; data regarding intellectual property; and data regarding industrial plants and machinery. As a general rule, the bigger an organisation's number of assets that are linked to the Internet, the greater the level of cyber risk it faces (CCCS, 2020: 21).

In the year 2020, the CCCS (Cyber Centre) published its report on the National Cyber Threat Assessment. This public study, which is based on sources that are classified as well as those that are not classified, examines current trends in the environment of cyber threats, the chance that these cyber threats will materialize, and how Canadians might be affected. The second version of their unclassified assessment makes the following observations: the number of cyber threat actors is growing, and they are becoming more sophisticated; cybercrime will almost certainly continue to be the type of cyber threat that is most likely to affect Canadians; ransomware attacks will almost certainly continue to target large enterprises and critical infrastructure providers; and cybercrime will almost certainly continue to be the type of cyber threat that is most likely to affect Canadians. According to the findings of the Centre's investigation, there is an extremely high probability that state-sponsored actors will keep making attempts to steal intellectual property and proprietary information from Canada, particularly material linked to COVID-19.

In addition, the analysis reveals that the actors are very likely striving to acquire cyber capabilities to disrupt the infrastructure of Canada, such as the delivery of energy, in order to achieve their objectives. On the other hand, they concluded that it is highly improbable that state-sponsored actors would purposefully impair Canadian essential infrastructure in the event that there were no international wars. These findings shed light on the severity of the threat that digital attackers pose to Canadian businesses and the customers those businesses service. This is something that has been brought to the attention of the Canadian Centre for Cyber Security, which is why they have developed the National Cyber Threat Assessment for 2020. This study, which is based on the unified approach to cybersecurity adopted by the Cyber Centre, gives Canadian policymakers, corporate leaders, and ordinary citizens the knowledge they require to defend themselves against the cyber dangers outlined in the previous section (Shariff & Bisson, 2021).

According to Bayne and Friesen (2017: 2), prior to this declaration and the consolidation of activities into a single harmonized Canadian Safety and Security Programme (CSSP), risk assessments were primarily based on ad hoc processes that were used by partner departments. This declaration and the consolidation of activities into a single harmonized Canadian Safety and Security Programme took place in 2017. These evaluations were made more difficult, and continue to be made more difficult, by certain mandates, regulations, and laws. Risk assessment responsibilities have been decentralized to individual partners or programme elements that were designed to respond to security threats, with terrorism being the most serious of these. With a few notable exceptions, where CSSP has played a lead role in facilitating multi-party threat assessments, these responsibilities have been assigned to CSSP. The inclusion of new areas of responsibility, such as emergency management, vital infrastructure protection, cyber security, and border protection (EM).

It has been noticed that South Africa and Canada have a lot in common when it comes to the safeguarding of their essential infrastructure against external influences. Cybercrime, cable thefts, and attacks on economic cities' power substations are all believed to have been committed by individuals who were not originally from South Africa. Both Canada and South Africa continue to have difficulty in implementing threat assessments that would allow for effective responses to acts of cybercrime.

5.27 SUMMARY

The chapter was dedicated to presentation and discussion of key legislations which form the conceptual pillars for the STRA in South African government departments. The reviewed pieces of legislations safeguard government departments from threats emerge from the social, political, financial, and technological environment. In this chapter, the researcher discussed the Constitutional mandate in ensuring that the security programmes are implemented in consideration of the democratic values of equality, human dignity, and freedom. In addition, it encouraged that the security practices should respect, protect, promote, and fulfil the rights in the Bill of Rights. However, the Bill further state that the rights are subject to the limitations contained or referred to in section of the Constitution, or elsewhere in the Bill.

The chapter included legislations that were inherited from the apartheid dispensation and have not yet been replaced to meet the Constitutional requirements. The researcher included case studies in selected legislation to emphasis their impact on protection of government departments' assets, information, and the people. Furthermore, the researcher discussed the Canadian legislation and challenges of cyber security in Canadian government for international comparability purposes.

In the following chapter, the researcher presents and discusses the research findings, recommendations, and conclusion.

CHAPTER 6

FINDINGS, RECOMMENDATIONS AND CONCLUSION

6.1 INTRODUCTION

The current chapter largely presents the findings, recommendations and conclusion accruing from the study. The findings themselves are necessarily a product of the thematically analysed data, which is consistent with analytic approaches that are usually implemented in qualitative research studies (Aurini, Heath & Howells, 2016: 12). The demographic characteristics or profiles of the participants are presented first for purposes of contextualisation, followed by the findings and recommendations.

The findings themselves are presented in accordance with each research question, in terms of which sub-themes were subsequently developed. It is important to note that every research question has its own findings which emanate logically from the aim of this study as articulated in Section 1.6, which is: To critically review the implementation of the security threat assessment by a selection of government Department in Gauteng.

From the viewpoint of the researcher, the afore-mentioned research aim or purpose statement of the study addresses various issues and aspects related to security threat assessment, and necessitated the identification of the relevant theories of security threat, risk, and vulnerabilities. In general, theories are useful for analysing, applying and determining the causes of ineffective implementation of security threat assessment and its impact on government departments (Trochimm, 2020 cited in Troy, 2020: 14). In that regard, it was imperative to consider reviewing the current mechanisms of protection in South African legislative, national policy, and regulatory framework to determine their efficacy; formulating and designing a more effective best practices in comparable jurisdictions and the researcher's experiences.

The recommendations in this chapter are intended to address the shortfalls and challenges in the South African Government departments in relation to implementation of the security threat assessment as explored in the literature and qualitative research, and eventually improve the field of security in government. Furthermore, this chapter covers the limitations and contributions of the study, as well as the proposals for future research.

6.2 DEMOGRAPHIC CHARACTERISTICS OF PARTICIPANTS

Table 6.1 below is a representation of the study participants' demographic characteristics.

Table 6.1: Demographic details of participants

Participant Code	Gender	Specialisation	Title/Rank
Participant 1	Male	Digital forensics and cybercrimes	Investigator Cybercrime
Participant 2	Male	Physical security and Vetting	Security Manager
Participant 3	Female	Physical security	Security Manager
Participant 4	Male	Physical security	Security Manager
Participant 5	Female	Information security	Assistant director
Participant 6	Female	Information security	Assistant Director
Participant 7	Female	Vetting specialist	Assistant Director
Participant 8	Female	Information security	Assistant Director
Participant 9	Female	Information security	Assistant Director
Participant 10	Male	Vetting investigation	Assistant Director
Participant 11	Male	Security Manager	Assistant Manager
Participant 12	Male	Security risk managements	Assistant Director
Participant 13	Female	Cyber security	Assistant Director
Participant 14	Male	Cybersecurity	Assistant Director
Participant 15	Female	cybersecurity	Assistant Director
Participant 16	Male	Security, specialisation Protection Services	Security Manager
Participant 17	Female	Vetting	Security Manager
Participant 18	Male	Vetting Investigator	Sergeant
Participant 19	Male	Assistant Director	Forensic Investigation and Auditing
Participant 20	Female	Vetting specialist	Vetting investigator
Participant 21	Male	Physical security	Assistant Director
Participant 22	Female	Vetting specialist	Manager
Participant 23	Female	Vetting specialist	Assistant Director
Participant 24	Male	Vetting specialist	Assistant Director
Participant 25	Male	Physical security	Assistant Director
Participant 26	Male	Physical Security	Assistant Director
Participant 27	Male	Digital forensics and cybercrimes	Investigator Cybercrime
Participant 28	Male	Physical security and Vetting	Security Manager
Participant 29	Female	Physical security	Security Manager
Participant 30	Male	Security Management	Security Manager

Source: Researcher's own compilation

The researcher managed to draw data for each research question from participants until saturation was reached at the 30th participant. Extrapolated from Table 6.1 is that the majority of participants (n=17, 57%) were male, whereas females constituted a minority (n=13, 43%). Also evident is that all the participants (n=30, 100%) were from the security sector, and occupied various security-related positions in their employment. Therefore, their involvement in the study lends credence to the researcher's judgement in their selection (Aurini et al., 216: 13; Efron & Ravid, 2019: 27).

6.3 CONTEXTUALISATION OF KEY FINDINGS

From the researcher's perspective, the contextualisation of the key findings logically distinguishes the findings themselves on the one hand, as well as the perennial intersection of the secondary and primary data throughout the chapters of the entire study. In that regard, the findings themselves are presented as the cumulative outcome of both the literature-based perspectives and participant-specific contributions that have emerged in varying degrees and contexts throughout this research process (Kumar, 2019: 118; Majid, 2018: 22).

Accordingly, **Chapter 1** contextualised the study by demarcating and outlining the research problem, research objectives, limitations and research questions as well as research design and methodology. provides an overview of the entire study. However, this chapter indicates that some of the machinations of hollowing-out and weakening the capacity of the affected departments included (Surju, 2018: 12-13):

- extensive corruption at the Executive level throughout all organs of the State;
- factional politicisation of the intelligence, policing, and prosecution system; and
- vulnerability in governance due to re-purposing of departmental mandates.

In **Chapter 2**, the researcher discussed various points regarding the concepts of risk and threat. In addition, the term "opportunity" is defined as an upside risk that results in positive effects, whilst the term "threat" describes an upside risk that results in negative repercussions. Furthermore, many departments have difficulty adopting STA, which requires them to look for opportunities within the risk process. The researcher noted in Chapter 2 that opportunities have a greater potential to have an effect on the level of threat than any other component. However, those in charge of maintaining security might exert a significant amount of control over opportunities by closely monitoring the vulnerabilities of assets (Thoka, 2020: 14).

The degree to which certain assets require protection from threats would vary depending on the nature of a department's primary business and the significance of the business to South Africa's national interest and national security. As such, these consequences are essential for the department's evaluation of potential threats and risks with a comprehensive understanding of the department's primary core business, and proceed to identify the most essential vital assets that will need to be protected. Critical assets are the departments' essential business operations, staff and clients, information technology assets, physical infrastructure, services, as well as intangible assets (Katsikas, 2013: 23). These directorates are identified as critical assets and should collaborate to identify the personnel who are high-risk and mostly using these assets.

Chapter 3 presented and discussed threat assessment in the context of the underlying causes of a security vulnerability and the development of controls (physical, technical, and operational) to prevent, postpone, and reduce the negative effects of an incident on the departments. In Chapter 3, vulnerability relates to a breach that can be detected in the current security mechanisms (Watts, S. 2017). The security vulnerability assessment does not only provide senior management with evidence that vulnerabilities do exist but also contributes to the process of acquiring cash for potential solutions.

Since risk is often difficult for security practitioners to describe, the researcher explains it in **Chapter 4** by mentioning that security risk is a key concern, and its explanation should utilise language that conveys uncertainty, such as might or might not, could or could not. As a consequence of this, the terminology should make it easier for security managers to describe the risk to security. The fact that it can only take place in the presence of the security threat, gives rise to the term dependency or contingent language. However, risk originates from someplace, that there are different courses of risk, and that management commonly confuses the course of risk with the real risk (Dalziel, 2015: 18). This is yet another important point that should be kept in mind. Therefore, one method for locating the security risk is to have a structured description that lays out the cause, the danger, and then the consequence; this is something that can be accomplished by making efficient use of the STA.

In **Chapter 5**, the researcher discusses the South African legislations and national policies that support the government security programmes. The chapter further discussed the Canadian Threat Assessment perspective and the challenges on cyber and digital crimes for international comparability purposes.

In **Chapter 6**, the findings and their context are presented and discussed in respect of the research questions as articulated in Section 1.8 of Chapter 1. The following sub-sections are a synoptic encapsulation of the overall findings of the study.

6.3.1 Risk Consequences

Assessment of threats and risks in the criminal justice system has a long and chequered history, dating back to the early 1900s when correctional officers relied on their own professional judgments to determine, whether an individual was likely to comply with the parole’s conditions (SAPS, 2011). Actuarial calculations are employed to categorise persons and adapt the reaction of the legal system in order to maximise the likelihood of desired results, hence the evaluations in the modern era are both more exhaustive and methodical in their approach. This transition from making informed "guesses" to evidence-based assessments occurred over the course of several generations of STA development, which are detailed in Chapters 2 and 4. Security professionals and policymakers be better able to contextualize the value and utility of current STA tools in increasing the consistency and efficacy of counterintelligence operations, if and only if they had a better understanding of the historical backdrop (Williams, 2017).

Cyber threat actors are able to hold information for ransom, sell it, or exploit it to obtain an unfair competitive advantage, according to research that was conducted. This poses a risk that might have serious implications. Attacks using ransomware and targeting industrial processes have become increasingly common over the past few years (Accenture, 2019). These attacks have significant repercussions, including a negative impact on reputation, a reduction in productivity, potential legal repercussions, increased costs for recovery, and damage to infrastructure and operations.

6.3.2 Digital Attacks and Information Theft

It has been discovered that in the absence of international hostilities, it is improbable that State-sponsored actors will purposefully impair Canadian vital infrastructure. This finding was revealed on the basis that it was unlikely for international hostilities to occur. These findings shed light on the severity of the threat that digital attackers pose to Canadian businesses and the customers serviced by those businesses service (Bayne, 2020: 38).

It has been discovered that cyber threat actors also imperil the information of firms, such as intellectual property and customer and client data (Accenture, 2019). Theft of this information could have major impact as well as long-term repercussions for the victims' finances, including implications on the victims' worldwide competitiveness and reputational harm (Hayes & Drury, 2019: 14). It has been discovered that organisations control a wide variety of assets that are of interest to cyber threat actors. These assets include intellectual property, financial information and payment systems, personal data of customers, partners and suppliers; as well as information about particular industries and machinery (Bayne & Friesen, 2017: 17).

6.4 MAIN FINDIGS AND THEMATIC CATEGORISATION

While they endorse the efficacy of the methodological processes applied in the study, the main findings are also indicative of the relevance and congruence of the research problem, aim and questions in relation to the research topic (Majid, 2018: 37; Ruel, Wagner & Gillespie, 2016: 17). It is particularly in the latter context that thematic data analysis was also applied according to the sequence and logic of the following research questions as articulated in Section 1.8 of Chapter 1. In addition to providing a framework for the dissemination of the findings (Ruel et al., 2016: 17), these research questions also facilitated the process of unbundling or dissecting the fundamental issues, concepts and knowledge pertinent to security threat assessment, theories of security threat, risk, and vulnerabilities, its causes and effects, and its impact on government departments; as well as factors that will have a direct influence on formulating and designing effective and efficient STA model.

6.4.1 Theme 1: The Scope of Government's Security Threat Assessment (STA) Framework Guidelines

The findings in the above regard are in congruence with the following requestion of the study, namely: **Research Question 1: What is the scope of government's Security Threat Assessment (STA) framework guidelines?**

The study sought to understand the participants' awareness of the STAF and its scope. The majority of participants demonstrated awareness of the framework, resulting in the emergence of the following key themes:

6.4.1.1 Role of Threat Assessment Framework Guidelines

The majority of the participants acknowledged that South Africa faces several threats including corruption, policy misrepresentation by senior executive in relation to asset classes if people, leak sensitive information, recruitment by human resource management in relation to asset class of core business process and intrusion of operations of intelligence in relation to asset class of people. In order to address these threats, most participants felt that the STA was necessary to mitigate these threat challenges. The following statements are from the majority of participants regarding the role of the threat assessment framework guideline:

Participant 1: *A threat assessment is a procedure that is fact-based and systematic, with the goal of identifying, investigating, evaluating, and managing potentially dangerous or violent situations. One of the most important objectives is to differentiate between a person who makes a threat and one who poses a threat. The purpose of the threat assessment is to locate weak spots within the asset class, the information, and the employees.*

Participant 2: *The Threat Risk Assessment Is carried out in line with the South African Police Service mandate. The division provides a wide range of services, such as lodging and property management, with the objectives of enhancing the built environment and attaining the objectives of poverty reduction. The Chief Directorate Security Services is concerned about the safety of personnel, as well as the security of valuable property and private information. This concern extends to the protection of staff. The Chief Directorate Security Services is obligated to make every effort to achieve compliance with the Minimum Information Security Standards (MISS), intelligence, physical security, and any other applicable legislation. This is something that the Chief Directorate Security Services is required to do.*

Participant 3: *The Chief Directorate of Security Services is susceptible to security risks and threats as a result of the nature of its mandate. These risks and threats can either put the Chief Directorate of Security Services' ability to effectively function at risk or cause disruptions in the performance of its primary business function. The STA is seen as a tool that can assist the department in evaluating the gaps regarding the current security measures, and this is something that the department views as being a potential use for the instrument. The effectiveness of the government's efforts to protect human lives, information, and property can be improved as a result of this factor. In an effort to provide assistance, Security Management Services and Key Account Management (Prestige) have been brought on board. The department's primary business statements are going to be assessed, and the results, together with the TRA's mitigation strategies, are going to be provided to the SSA Security Advisor who was assigned to the department.*

Participant 4: *After the stage of threat assessment has been finished, the structure of the plan to defend the core business of the department can be formed so that it can be put into effect. The plan should include a variety of milestones to help the department transition from the disruption position it is now into normal operations as quickly and efficiently as possible.*

Participant 5: *The goal of carrying out the threat risk assessment is to evaluate the dangers that are connected to the security measures that have been put into place in the department, as well as to identify the weaknesses that have an effect on the security measures that are currently in place.*

Participant 7: *Assessments of security threats and risks are carried out by both the SAPS and the SSA for the goal of providing advice services about risk reduction. This contributes to the department's efforts to downplay the severity of the threat. The conclusion of the evaluation has a direct bearing on the implementation of the Security Policy, which is a component of the overarching strategy for the department. The department does not currently have an authorised security police force, although there is a policy that is still in the design stage.*

Participant 14: *Understanding the fundamental aspects of the department's primary function is essential to developing an effective threat assessment and security strategy. While it is crucial to have a general grasp of potential dangers and loopholes, it is even more vital to be familiar with those that could affect a particular division. In order to design department-specific security policies and procedures, security assessment strategists need to determine how much effort, time, and money will be required.*

Participants 15, 23 and 29 concur that: *Everyone who works for the Department, including temporary workers and contractors, as well as anybody who visits the Department. In addition to that, this is going to cover the following: protective security, security administration, security organisation, physical security, information security, personnel security, information and communications technology security, and BCP.*

The strategy should also be applicable to all of the Department's different types of facilities. Participant 29 also mentioned that the scope of this exercise encompasses the entire department at the head office level, and that it will be distributed to regional offices in instances where risks that are comparable are found.

Participants 10 and 11 agree that: *An application's critical security controls can be identified, evaluated, and put into place with the help of a security threat assessment. In addition to this, it places an emphasis on the prevention of application security flaws and vulnerabilities. An enterprise has the ability to observe the application portfolio in its entirety from the point of view of an attacker when they do a risk assessment.*

Participant 12: *The first step in the security threat assessment strategy is to determine the value of the department's assets. Next, we look at the threats that might prevent the department from fulfilling its service delivery mandate if such assets as buildings, machinery, electronic equipment, and personnel can be stolen, vandalized, or harmed. Finally, we assess the seriousness or likelihood of such threats materializing based on the efficiency of the department's existing security measures. After going through a consultation process, this data is then used to inform the department's security policy.*

Participant 13: *The Concept of STA Security Strategy provides a definition of information assurance and security initiatives, as well as a priority ranking for these initiatives, which the department is required to initiate in order to increase the safety of information and related technologies. After that, the department's objective and vision should be supported by the security policy, which should also include information that makes it obvious what needs to be secured.*

Participant 27 shared **Participant 16's** similar views as well as **Participant 29:** *To perform this threat assessment task, it is necessary to assess the security risks associated with a particular site. It covers a wide range of risks, such as: natural threats (including tornadoes, hurricanes, floods, earthquakes), criminal threats (such as theft from a location, violence against employees), terrorist threats (such as active shooters, vehicles, and person-borne improvised explosive devices), as well as potential accidents.*

Participant 30: *Security Threat Assessment is a sub-category of Security Risk Assessment. The latter briefly entails:*

- *Asset Identification & Categorisation – (High valued / critical assets, e.g., value of substation versus value of vehicle). This further entail Consequences/ Impact Assessment in respect of Legal, Financial, Reputation, Stakeholder & Customers, and other factors*
- *Threat Assessment - (identify and assess adversaries - insider versus outsider threats and their intents, capability & history of manifestation)*
- *Vulnerability Assessment – identification and characterization of adequacy of existing security controls, their degree of effectiveness to reduce vulnerabilities and / or to mitigate damage to assets in the event of attack by a threat agent.*
- *Risk Assessment _ often represented by Probability X Impact, estimate the degree of impact relative to each asset, estimate likelihood of attack by threat agent, estimate likelihood that a specific vulnerability will be exploited.*
- *Security Countermeasures Assessment – This is the last stage which prioritises security measures to be implemented, bearing their return on investment, trade-offs, and their value to achieve the Delay, Deny, Deflect, Devalue, Detect, Respond & Contain security principles.*

In the context of security policy development, the above process becomes an input, and provides a broad policy statement on the security philosophy the organisation will adopt to manage security risks. In the context of security strategy, the security risk assessment process provides an input in respect of the risks the organisation is facing, and the necessary strategy and plans required to manage same (Surju, 2018: 47).

Based on the responses from participants regarding the role of STA, the researcher noted that most of the participants were aware of the STA and its role and the objective thereof. One of the key ideas raised by participants was that the STA should eventually be leading to policy formulation, which at the present moment, is not there. In summary, the participants identified the following as the role of STA:

- To assess the effectiveness of existing security measures;
- To identify, inquire, assess, and manage potentially dangerous or violent situations;
- To identify weaknesses in the current mechanism of protection;
- To mitigate threats against the departments;
- To support the development of security policy should then support the mission and vision of the department;
- To determine the value of assets in possession of the department; and
- To direct the policy document on how these properties should be protected.

Based on the views expressed by participants, the STA is an important framework as a directive to identify security concerns, the value of state assets, and ways to reduce potential dangers. It is noteworthy that the absence of a security policy completely nullifies the STA’s prospects (Kabanda et al., 2017: 7). All participants concurred that STA is about protecting the assets, information, and the people.

6.4.2 Theme 2: The Role of Other Directorates in Implementing the Security Threat Assessment Framework

The findings in the above regard cohere with the following requestion of the study, namely: **Research Question 2: What is the role of other Directorates when implementing the Security Threat Assessment Framework?**

Regarding the role of other (non-security related) directorates in implementing STA, the participants identified different roles that the directorate is involved in. Most of the participants indicated that the directorates give direction and oversight to implementation of STA. The participants indicated that the directorate have the following roles:

6.4.2.1 Ensuring Security Management

The Department has identified an inadequate compliance with the National Policies such as the MISS document (1998). The inclusion of other directorates provides expertise in identifying critical assets and knowledge of who is authorised to gain access to sensitive information. To mitigate these security threats, the participants indicated the following with regards to the role of the directorate:

Participant 2: *It is the responsibility of all personnel to protect the information and the assets of the department. However, the overall security risk management is a primary responsibility of the Directorate Security under the security manager on the level of Director. The component should have a vetting field unit, cybersecurity, information security, and physical security that has memorandum of understanding with the SSA, and in line with the DPSA.*

Participant 4: *The development of security policy requires the participation of all directorates. The first important milestone is the process is developing a security policy that is going to support the primary mandate of the department. That means the critical assets that contribute to the success of the core business of the department must be clearly identified.*

Participant 13: *The context of STA is to protect the primary mandate of the department and directorate security plays the supporting role. There are other departments that makes the department what it is, and the Security Manager should must be able to consult with all heads of directorates to implement a successful STA.*

Participant 20: *The sensitivity of information that is generated by other directorate on official capacity, and the consequence of landing such information in hands of aggressors is known by people who generates it, not directorate security.*

Participant 27*: Non-compliance by some directorates with the vetting and screening of companies poses a potential threat to some of the projects undertaken by the department as some companies have proven to be incapable of delivering on the projects, after the vetting process has been ignored.*

6.4.3 Theme 3: The Role of Management in Supporting the Security Programmes

The findings in the above regard relate to the following requestion of the study, namely:

Research Question 3: What is the role of management in supporting the security programmes?

The study sought to understand the participants' views concerning management's role in respect of supporting security programmes of the STAF and its scope. The majority of participants demonstrated awareness of the framework, resulting in the emergence of the following key themes:

The participants expressed the following perceptions regarding the role of management:

Participant 1: *A Security Management System may be considered as that part of the overall management system, based mainly on the quality management system, provides the structure to enable identification of potential threats to the department and which establishes, implements, operates, monitors, reviews and maintains all.*

Participant 2: *The head of the departments must delegate their duties to the head of all business units in a form of security committee, to ensure that they provide guidance to the security component in order to align the security policy with the overall strategic pillars of the departments. The security policy should communicate directly with what the departments seek to achieve in their business plan.*

Participant 5: *The security manager responsible for protecting the assets, information, and the people on behalf of the Accounting Officer should consult with all the heads of business units and the stakeholders in order to clear define the core business of the department and identify the critical assets of the department.*

Participant 7: *Security structure is established to protect the assets of the department, the personnel and client, and the information of the department. Therefore, the structure should be led by a qualified and experienced manager on a level of Director in possession of NQF Level 8. The operational scope of the component should be directed by the primary mandate of the department. The component should cover physical protection, security personnel, information technology, and information security, and all these unit should be led by a Deputy Directors in possession on an NGF level 7.*

Participant 11: *The security manager who will oversee the structure must be chosen by the department. The senior management is responsible for ensuring that STA strategies are in place as well as supporting the security programme. Management is responsible for ensuring that STA recommendations are carried out efficiently and on schedule.*

Participant 13: *The HOD delegates the duties of developing the security policy to the security manager, who then includes all stakeholders to participate in the drafting of the policy. The policy should a piece of laws that indicates how it is going to support the core business of the departments, whilst maintaining the security principles of prioritizing the safety and protection of employees and visitors, critical infrastructure of the department, and the classified information produced on official capacity.*

Participant 16*: The misrepresentation in policy development and corruption by Senior Executives of the departments, has been damaging to the departments' reputation and has created obstacles to local and foreign direct investment, flows to the stock market, global competitiveness, economic growth and has ultimately distorted the development of South Africans. It has a direct impact on public money that is allocated for government services and projects.*

6.4.3.1 Role of Management

Based on the views expressed by participants, the main function of management is overseeing the development of security policy, security committee and appointment of security manager. However, **Participant 16** highlighted the concern of corruption and management's inability to direct policies. Just as directorates, management plays a crucial role in supporting security programmes. Most of the participants were aware of the role of management and some of the roles that were identified by most of the participants include: management of the overall security management system; delegating duties; protecting assets; sensitive information; and people ensuring that

STA strategies are in place and implemented. This perspective is in agreement with the observations made by Bickley (2017) in this regard.

6.4.4 Theme 4: The Processes for Appointing the Security Manager and the Security Committee, and Their Respective Roles in Threat Assessment

The findings in the above regard are congruent with the following requestion of the study, namely: **Research Question 4: Which are the processes for appointing the Security Manager and the Security Committee, and what are their respective roles in threat assessment?**

The participants provided the following perspectives relating to the process of appointing a security manager and the security committee, as well as their respective roles in threat assessment:

Participant 5: *The MISS document provides guidance on how to protect the departments and the responsibilities of the Head of the department. Security structures should consult with the SSA to assist structuring the security component. The security component is led by a director, who is the security manager and the automatically the chairperson of the security committee.*

6.4.4.1 Processes of Appointing a Security Manager and the Security Committee

The majority of participants indicated that they had knowledge of the process of appointing a security manager and the security committee. The participants indicated that the appointment should be informed by the size of the department and the protection needed by the department. Notably, the identified threats guide the strategic objectives of the committee (Black, 2010).

6.4.4.2 Roles of Security Manager and Security Committee

Apart from identifying the appointment processes, participants were asked to provide their views relating to the roles of security manager and security committees. Most of the participants demonstrated awareness of the functions of these two portfolios. This finding coheres with the same observations by Brotby (2008) and Dalziel (2015). Three key thematic issues were identified by participants in terms of the role of security manager and security committee namely, the strategic direction, security component, training, and development.

6.4.4.3 Strategic Direction

Relating to strategic direction, the participants commented thus:

Participant 2: *The role of committee is to provide a strategic direction and ensure that the implementation of the threat assessment is conducted yearly and when threat is identified.*

Participant 14: *It is the responsibility of the Security Committee to provide direction on when and how the STA can be implement and who should be included in the team to ensure that* *the assessment cover all the departments' business unit and the core business of the departments.*

Participant 15: *The responsibility of the security committee includes but not limited to the oversight of: Security arrangements for events both in and out of the building, any other areas that relate to the security of the building, review of activity logs of security personnel on a weekly basis.*

Participant 30: *A security committee is an important governance structure that provides assurance to Executive Committee and/ or Board that risk and threats facing the organisation are proactively properly managed. Broadly, the purpose of a security committee is to provide a company-wide governance structure and oversight over security management by ensuring that security risks are properly identified, and appropriate security measures are implemented to mitigate security vulnerabilities, risks and threats to acceptable risk levels.*

6.4.4.4 Security Component

Participant 6: *Security component shall be responsible for the safeguarding of personnel, assets, and information by executing access control Twenty-four (24) hours per day, in terms of the Control of Access to Public Premises and Vehicle Act, 1985 and National Key Point Act 102 of 1982. Contract security personnel may be appointed on contract after the invitation of quotation or tender were approved by Bid Adjudication Committee to assist departmental security personnel in performing specific duties as prescribed by the Security Manager. Strict control measures must be in place to control and monitor all contracted security personnel.*

Participant 13: *Security component is managed by the Security Manager on a level of Director and supported by the Deputy Directors for Vetting, Physical Security, IT Security and Mission Security. The component's responsibility is to manage the total Security function in the country and abroad, ensure safety and security for all department's facilities, implementation of Security and Risk Management, implementation of vetting, screening and compliance with prescripts, monitoring the implementation of Occupational Health and Safety and ensure implementation of security measures in consultation with the SSA and SAPS.*

Participant 30: *The strategy ought to come before the structure. The plan ought to be informed by the macroenvironment (a PESTEL or SWOT analysis), internal organisational capabilities, and the security risk assessment procedure described earlier in this paragraph. The majority of departments make the error of believing that all firms adhere to a universally established security structure. The structure of something cannot be managed in any way. Instead, management should be focused on the strategy, which is supposed to be managed because strategies are what provide value for the department and help in achieving strategic goals and objectives. Therefore, structure is what drives strategic decision-making.*

6.4.4.5 Training

Participant 13: *The security manager should have responsibility for on-going maintenance of security procedures and training and can help devise and implement your training regimen. The security manager, with the support of the security committee, should ensure that the employees receive the appropriate training on how confidential information should be stored in order to achieve the highest possible level of protection. They need to ensure that the MISS implementation is carried out throughout all government departments, and then evaluate how effective it is.*

From the perspectives presented by participants, the study stabled that participants understand the roles of the security manager and security committee. In addition, by giving the manager and committee leadership roles, they are better positioned to oversee deficits in security and recommend policy and identify training needs, in agreement with perspectives posited by Surju (2018: 38).

6.4.5 Theme 5: The Departments' Processes of Anticipating and Analysing the Probabilities of Loss and Damage to State Property

The findings in the above regard are congruent with the following requestion of the study, namely: **Research Question 5: Which are the Departments' processes of anticipating and analysing the probabilities of loss and damage to State property?**

Most of the participants did not fully articulate the processes involved in anticipating and analysing possibilities of loss and damage to state property. This may indicate lack of awareness with requisite security documents such as a MISS. Therefore, the participants identified the security component as a key role player in ensuring that threats are identified, and measures to counter these threats are taken. The participants commented thus:

Participant 1: *The basic risk control strategies are defence and prevent the exploitation of the vulnerability. This is accomplished by countering threats, removing vulnerabilities in assets, limiting access to assets, and adding protective safeguards. This approach is also referred to as avoidance. There are four main risk management strategies, or risk treatment options: Risk acceptance, Risk transference, Risk avoidance and Risk reduction.*

Participant 18: *The security committee should play an oversight role to ensure that security policies, procedures, strategies, and measures are implemented to protect the assets of the departments or institutions against potential threats and risk. To monitor and evaluate the effectiveness of the security measures in place. Ensure that continuous security assessment is conducted as the crime is not static.*

Participant 30: *The department conducts security surveys or vulnerability assessments, during which they detect adequacies or vulnerabilities in the existing security measures, and then they recommend a variety of security solutions such as access controls, CCTV cameras, protocols, and so on. This procedure is deficient due to the fact that it does not identify, evaluate, or prioritise assets. Furthermore, it does not investigate threats and threat agents' intentions, capabilities, or history of events.*

In many cases, security is handled independently from the department rather than as a key enabler of overall strategy. As a direct consequence of this, the vast majority of security functions and departments are unable to successfully establish themselves at the core of their respective businesses. As such, the majority of security strategies are still focused on the conventional approach. These measures are regarded more as cost centres than value increases (Fay & Patterson, 2018).

6.4.6 Theme 6: Current Layers of Security Measures

The findings in the above regard are congruent with the following requestion of the study, namely: **Research Question 6: What are current layers of security measures?**

Few participants responded directly to this aspect, which may indicate lack of awareness about the layers of security measures that are deployed by the department. What most participants mentioned was the MISS and vetting processes. Following are the responses from the participants:

Participant 1: *Minimum Information Security Standard (MISS) was compiled as an official government security policy document, which must be maintained by all departments to physically protect the assets, information and the people. The document further provides guidance on how to handle sensitive/ classified material produced by the department on behalf of the government. This is meant to ensure that the national interests are protected.*

Participant 2: *The Department through the assistance of the State Security Agency (SSA) has identified unauthorised disclosure of information as a key threat to the department's ongoing projects especially in the prestige. The department has implemented the national vetting strategy to ensure that all new employees that enters the government departments go through the Personnel Suitability Checks*. *The department further ensure that all the personnel and clients are obliged to adhere to the MISS document.*

Participant 7: *The Minimum Information Security Standard (MISS) and the National Vetting Strategy should be applied to ensure that all management and specialists in critical positions are vetted. This would ensure the credibility of people who are entrusted with classified information.*

Participant 20: *A high-level document for proposing security structure related to threat risk assessment should be compiled. It should contain the plan as to why the organisation should invest in security threat risk assessment unit and it should provide a direction that is aligned to the business vision, mission and objectives.*

Based on the participants' views above, the conclusion would be that the MISS document is not fully understood by all personnel, but the participants are aware of the role of the document. Fay and Patterson (2018) concur that government employees are cognisant of security protocols, but ignore them at times.

6.4.6.1 Classification of Information

The security policy should clearly define the powers, responsibilities, and duties of security personnel, and all personnel are expected to adhere to the security measures (Gumedze, 2008: 18). Security is an essential component of management, and the security component's composition should be such that the line of authority does not obstruct access to top management.

6.4.6.1.1 Understanding the term "document"

In terms of the Protection of Information Act (Act 84 of 1982) a document is:

- any handwritten or printed note, plan, picture, sketch, photographic or other representation of any place or article; and
- any disc, tape, card, perforated roll, or other device in or on which sound or any signal has been recorded for production.

6.4.6.1.2 Considerations in the classification of documents

The following considerations are applied in the classification of documents.

Restricted documents are those that are classified on the basis that they contain information that could be used to embarrass an individual or institution by aggressors. Compromisation of such information could cause embarrassment to the integrity or reputation of an individual or departments (Mahlatsi, 2019: 14).

Confidential documents are those that are classified on the basis that they contain information that could be used by aggressor elements to harm the objective purposes or functions of a department (Renfroe & Smith, 2016: n.d.). When such information is compromised, it could lead to the following consequences:

- the disruption of ordered administration within the departments, and adverse effect on the non-operational relations between the departments;
- the embarrassment or damage to the integrity or reputation of an individual;
- the ineffective functioning of an information or operational system; and
- the frustration of the effective functioning of either system.

Secret documents are those that are classified on the basis that they contain information that could be used by aggressor elements to disrupt the objective and functions of the departments (Renfroe & Smith, 2016: n.d.).

6.4.7 Theme 7: Possible Solutions for Addressing Correct Implementation of Security Threat Assessment

The findings in the above regard are congruent with the following requestion of the study, namely: **Research Question 7: Which possible solutions could be implemented to address the correct implementation of security threat assessment?**

The participants made various suggestions based on how security threat assessment could be effectively implemented. Several strategies were suggested and are presented below.

Participant 5: *The department should ideally consolidate previously identified and executed projects, provide scope and definition for each of the identified efforts, detail the general risks addressed by the initiative, and provide a foundation that can later be refined by senior management. Furthermore, the security strategy planning process must identify any significant dependencies associated with the initiative in order to support higher-level evaluation of initiatives that can be undertaken when necessary. The security policy should then support the mission and vision of the department with a clear information of what need to be protected.*

Participant 10: *Security threat assessment strategy entails determining the value of assets in possession of the department, then also looking at the threats that might negatively affect the department from realizing its service delivery mandate if such assets including buildings, machinery, electronics and personnel can be stolen, vandalized or harmed, then we also look at the seriousness or likelihood of such threats materializing based of the effectiveness if current security measures. This then informs the security policy of the department after consultation process.*

Participant 14: *STA is the professional use of a systems approach, comprising accurate diagnosis, an aligned protection strategy based on sound theory and security principles (inference), and a mitigation system (treatment) that fulfils operational requirements accordant with legislation, standards, and engineering practice to manage the protection of assets, information, and personnel from damage, loss, or unauthorised access against internal and external threats.*

Participant 30: *STA is defined as one critical function within department. Secondly, security strategies should be based on comprehensive assessment of the department's goals, strategic objectives and the security risks emerging therefrom. Finally, the security function should regularly conduct security risk assessment, and the reports should input into the broad security strategy of the department. Security risk or threat assessment reports computed as standalone activities and failing to demonstrate value to the department hardly receive support and financial investment from management*

6.4.7.1 Wellness Centre

Employee wellness is a critical factor, especially in the government security sector (Duff, 2010: 3). To that effect, most of the participants shared the view that wellness practitioners help to detect mental health challenges that employees might be confronted with and help them before the condition pose a threat to the department (Cockerham, 2016: 17). The participants shared the following sentiments in relation to the inclusion of mental health practitioners in the implementation of threat assessment:

Participant 1: *It is the Employee Wellness Centre that should detect signs of employee depression and threats pose by how they handle their stress. the EWC also work in the secret setup that allows them to know the information that the management and security does not know.*

Participant 2: *Mental health practitioners work with personal things and should not be involved in security practices to determine information value, identify and prioritise assets, identify threats, identify vulnerabilities, calculate the likelihood and impact of various scenarios per year basis and employ the threat and risk assessment strategy.*

Participant 9: *Threat assessment should not be analysed only in context of security and intelligence, but also in a mental wellness of the employees. The employee wellness centre should be part of threat assessment team lead by the Security Manager.*
Participant 7: *Through the vetting policy, security component should ensure that the employee wellness is included as part of the recommendations when the vetting unit identifies issues that relate to mental illness or act of endangers behaviour. The security clearance applicant should be referred to the mental care for support.*

Participant 4: *The EWC can assist when threats emanate from domestic violence, mental health issues, as a support directorate, not really involved in the implementation of threat assessment.*

Participant 10: *A person before assuming responsibility in a security graded area should be accessed by professionals to determine their emotional and mental health.*

Participant 13: *In my view, the greatest threat to cybersecurity is not technology, but rather the human mind. Ransomware, viruses, and other malicious tactics used by cybercriminals frequently rely on a victim clicking a link or attachment in an email, using an easy-to-guess password, or unwittingly disclosing personal information. The wellness centre to close a gap on human behaviour and provide security with information.*

Participant 17: *Part of experience includes vetting and compliance, and Employee Wellness Centre (EWC) plays a very vital role in assisting the process with applicant with metal problems. Outcome of vetting sometimes suggest that an applicant is not mental stable and requires assistance, and vetting will make referrals.*

The relevance and importance of wellness came as a result of the observation that some employees may have mental health challenges, thus compromising threat to information and infrastructure under their control. The above responses indicate that the participants unanimously shared the view that mental health issues are a challenge at the workplace nowadays. As such, a wellness centre is helpful in resolving employee issues that could pose a security threat as a result of mental health concerns (Cockerham, 2016: 17). Additionally, departments could be vulnerable to internal threats by employees if they are not constantly checked for behaviour-related inconsistencies (Blanchard et al., 2010: 16).

6.4.7.2 Popularising the Minimum Information Security Standard Document (MISS)

From the interviews with participants, there was a concern regarding the awareness and implementation of the minimum information security standard document. Most of the participants felt that individuals who are in possession of sensitive information often mishandle it, resulting in private information breaches and related security threats. Regarding the popularisation of the MISS document, the participants commented thus:

Participant 2: *After the consideration of the probability of unauthorised access to information, in the form of prestige projects information, occurring given the media attention in this area* *and having considered the severe impact this will have in the entire prestige environment due to the lack of counter-intelligence training and awareness by the officials (project managers) in this area, the SSA has come to a conclusion that the department faces a major risk in this regard. Popularizing the MISS should be done through a policy development and monthly awareness programmes.*

Participant 9: *The department's intranet should be used to popularise the MISS document. Security should approach every business unit on awareness programmes and customise every presentation according to a targeted unit.*

Participant 14: *The MISS document should be the bible of every department to ensure that the employee understand the role of the HODs on security, the importance of protecting information and adhering to the vetting processes.*

Participant 20: *Security managers can play a crucial role in popularizing the Minimum Information Security Standard (MISS) documents. They can have road shows with different units, and they can invite an individual who knows and understands the contents of MISS. This can also be put in departments' intranet for easy access.*

Participant 30: *The MISS document should not be promoted because it is not a legislation, therefore it is not binding. The most critical gap in the MISS is the Personnel Security chapter 5 which outline the security vetting and screening process. The criteria outlined is outdated and require drastic review. It is very difficult for an ordinary employee including management to voluntarily buy into the process of vetting due to the lack of clarity of what it means to have a security clearance. Presently, the criteria is access to classified information. The latter is equally problematic because employees can hardly appreciate what classification of information mean in simple day-to-day terms.*

Based on the above views from participants the cases of security lapses are rampant in government departments. Most of these security threats are caused by lack of understanding for awareness about handling sensitive information, as confirmed by Blanchard et al. (2010: 16). The origin of the lack of awareness is the recruitment process. Participant 30 opines that the MISS document should be set aside, and the government should implement a legislation that is binding. Participant 30 further identified a gap in Chapter 5 of the MISS document.

6.4.7.3. Vetting

Most of the participants indicated security lapses as a major cause of security threats that the department faces. To that end, the participants indicated that vetting should be a priority in order to ensure that personnel who handle sensitive information are fit to do so. In the past, there have been cases of intrusion of intelligence in relation to the asset class of individuals (Hull, 2018). It is difficult to prevent every intrusion, but all should be detected to minimise impact to the department. The participants indicated that the department should facilitate the identification and development of vetting strategies and procedures in government departments. The participants commented thus:

Participant 3: *The Department has identified and considered the probabilities of fraud and corruption on tender, procurement, and leakage of sensitive classified prestige documents to the media, civil society groups, and political parties on departmental business processes. It was found, among other things, that the officials of the Departmental are colluding with services providers to defraud the department. All employees who are working with classified and sensitive information must be vetted, and that includes all management in the department because they are involved in corruption.*

Participant 4: *All employees working with classified information must be vetted.*

Participant 18: *There has been a problem of interference of labour unions when comes to vetting of employees. The vetting process has been misinterpreted and associated with invading of personnel's privacy, and therefore labelled "witch-hunting".*

Participant 5: *The department is currently subjecting the Contractors/consultants to the same vetting procedures as any employee of the department.*

Participant 11: *The vetting process should be able to aid the HR management processes at the departments, with favouritism and nepotism and abuse of authority in areas of recruitment, training, promotion and transfer identified as major risk areas. This is rendered possible by unchecked discretionary power, lack of integrity, accountability, checks and balances and transparency in the overall administration of HR services.*

The biggest concern that was raised by participants in relation to the need for vetting was the prevalence of corruption by government officials or individuals working on government projects. The study identified most threats that occurred in the department due to corruption activities by the Senior Executive, HR Officials, and all official who were able to access sensitive information. The corrupt decisions that are undertaken by the Senior Executives pose a threat to the core business of the department. As a result, policy documents cannot be approved, assets are unavailable, service cannot be delivered, and that has a negative consequence on personal impact of key employees (Imperva, 2021). The assessment further indicates that employees have low expectations on Senior Executives in terms of their relations and job satisfaction, as well as their knowledge of codes of conduct, anti-corruption policies and reporting mechanisms. This has a financial implication, and the department is at risk to suffer a financial loss, and legal liabilities (DPSA, 2016).

The findings further indicated that it is imperative for government departments to ensure that quarterly reports are provided. In these reports, they are expected to provide the following:

- The total number of officials that are vetted or not vetted in departments;

- The challenge here is always to tally between SSA vetting status and that of departments. The figures always do not tally/correspond;
- Obvious reason is that SSA has some challenges of their own in as far as capacity is concerned; and
- SSA has a huge backlog of vetting results that are outstanding countrywide.

The data reveals further that the department is responsible for identification and facilitation of vetting strategies and procedures. The participants admitted that the SSA is currently faced with a historical backlog of security vetting requests or applications from national, provincial and local government. In addition, one of the biggest problems which causes backlog is that departments have a tendency of vetting everyone/ all officials instead of focussing on certain categories first (Bickley, 2017: 30). Therefore, the participants were of the view that Security Managers should rather vet the majority of officials on Confidential Clearance level, which does not require much effort but only documents.

6.4.7.4 Securing Sensitive Information

The rapid increase in technology is beneficial but also comes with challenges related to the security of sensitive information. This was the overwhelming sentiment expressed by the participants. They indicated that the personnel working in high-risk environments as well as the ones in charge of information technology systems should be subjected to security procedures. These include: the use of Declaration of secrecy form; security profile of each user; limit access to top secrets to individuals who are towards retirement or exiting the system; and backup of the sensitive information in case it may be tempered with. The participants said the following:

Participant 5: *All information technology system users/contractors/consultants shall sign the Declaration of Secrecy and an Operator Undertaking Form. Copies thereof are placed on the user's personnel file. A security profile to control access to the institution's information technology systems is compiled for every system user/contractor/consultant. Key personnel/users in high-risk environment shall, when they state their intention to resign, be transferred to a lower risk environment. They shall not have access to sensitive and classified (SECRET or TOP SECRET) information for at least the last 30 days. Backup actions shall be in place in this regard and an audit trail shall be instituted on their actions.*

Participant 9: *All security breaches are reported using appropriate channels. All physical security breaches are reported to SAPS, and all information security breaches are reported to SSA. All this should be reported via the Security Managers. An approved security policy is implemented and well communicated through all business units. All candidates are pre-screened*

Participant 14: *A complete backup- backing up your entire hard drive. The advantage of this strategy is its completeness; you will get a snapshot of all your hard disk's contents.*

Participant 15: *Once the primary and secondary use cases for threat intelligence have been identified, the department should target accomplishable adversaries. This provides additional information about the adversaries' TTPs. Gathering knowledge of specific attacks and adversaries in the organisation's environment assists security teams in refining and improving protection mechanisms with threat intelligence.*

Participant 10: *The department should identify areas of sensitivity and before a person occupies the position in those areas, they should have a positive security clearance of a top secret.*

Participant 13: *Surveillance of the network's perimeter creates multi-layered boundary defences by deploying firewalls and proxies between the untrusted external network and the trusted internal network. Safeguard the internal network Protect internal IP addresses by preventing direct connections to external services.*

Participant 14: *It is almost impossible to over-emphasize the need for a good backup strategy. System backups not only protect the department in the event of hardware failure or accidental deletions, but they also protect staff against unauthorised or accidental changes made to file contents. If an error is ever made (and we all know that they are), having the option of accessing an unaltered backup can be very appealing. But reaching into those archives is a viable strategy only when backup files have been made properly- a backup of a file that contains the errors and/or viruses you are trying to eliminate usually isn't very helpful.*

From the views expressed by participants above regarding handling of sensitive data in the digital age, the study established that cybersecurity threats are some of the biggest challenges facing the department and most of the perpetrators are the individuals trusted with handling of the information and digital infrastructure. Apart from cybersecurity measures, the participants also indicated that the sensitive information should be secured using physical security mechanisms, in agreement with (Mdluli, 2011). These included deploying security personnel and fencing. The participants echoed the following sentiments:

Participant 12: *Most government departments and parastatals use physical security measures such as deploying security guards to provide guarding, access control as well as patrolling duties in all premises. This is complemented by security aids such as CCTV cameras, Bio-metric systems, turnstiles, X Ray parcel scanners, metal detectors, etc.*

Participant 21: *As a security objective, detection is not restricted to physical security measures like perimeter fence and alarms but applies to all the security programmes. The departments should apply a comprehensive security risk management process by introducing new physical security measures like CCTV cameras, bio-matric access control system, electric fence, and alarm systems.*

The study established that the department should put in place measures for the security of sensitive information using technology tools for the security of information stored in digital technologies, vetting personnel working with the technologies and providing physical security, as supported by Bickley (2017: 30).

6.4.7.5 Awareness

As indicated earlier, participants were of the view that some of the personnel do not know the importance of the sensitive information they handle. In addition, the personnel who were recruited through corrupt means may be poorly trained or lack skills to handle sensitive information. Therefore, according to the majority of participants, it is imperative to introduce awareness programmes for the personnel with a focus on these security issues (Bickley, 2017: 30). The participants echoed the following sentiments:

Participant 1: *Lack of awareness training that leads to officials susceptible to* ***bribery*** *has been noted by the SSA as a notable vulnerability that will prove to be a moderate hindrance at this stage but has a potential to escalate if unattended. My actionable strategy would invest in on-going training of security officials and ensuring that the cybersecurity personnel are updated with the ever-changing trends in information technology space.*

Participant 3: *Put the MISS awareness programmes in every security directorate's key performance area, and that includes vetting unit, physical security, and information technology security.*

Participant 4: *Security awareness programmes must be intensified and conducted regularly especially amongst senior personnel. The Security Manager assisted by the Security Committee must take the lead in the actual development, drafting and implementation of the plan (which will include marketing of the plan by means of the security awareness programme of the institution).*

Participant 5: *Information technology security awareness shall be provided to sensitise all employees in the Department. The awareness will be conducted by ICT Manager with the assistance of the Security Manager.An Institution's security awareness programme needs a successful launch for maximum impact. An awareness programme checklist can help ensure that the critical elements listed below are not overlooked: Awareness programme focus that security, at its core, is a people problem.*

Participant 7: *The security component should conduct awareness programmes on MISS as if it is an additional tool, but it should be included in their performance score card as a Key Performance Area. The MISS should be the bible of the department to ensure that the information, people, and the assets are protected by the personnel.*

Participant 11: *Having a policy is not sufficient; the hardest part is making sure it is put into practice. Employees should be aware of their responsibility in preventing security lapses and be aware of what to do in the event of one.*

Participant 12: *Awareness workshops can be an effective tool to indicate the importance of protecting information in government institutions through vetting and screening of personnel, safe storage of information, practicing office security, proper key control, so that people can know that they not being targeted for wrong reasons. It is a proper platform where they can then easily ask any question such as privacy issues etc.*

Participant 13: *I think awareness programmes and use of pamphlets. However, the security division expect the personnel to study the policy on their own personal capacity. Security department rarely conduct awareness programmes.*

Participant 23: *The first thing that comes to mind is awareness programmes. However, there are many things that the department can educate the personnel about the MISS, and that includes using of posters, department communications, and pamphlets. The department does not educate the personnel.*

The data shows that the majority of participants felt that awareness programmes were vital to ensure that all personnel become aware how to manage security infrastructure and information as well as the implication of security breaches. From the views presented, the study established that the security components do not prioritise the security awareness programmes. Therefore, the employees are not aware of what they should comply to.

6.4.7.6. Development of a Security Policy

From the interview data, there was a general consensus among the participants that apart from the STA, the department did not have a security policy in place. As a result, there was no clear roadmap or guidelines on the processes and procedures to address each security threat. Commenting on the need for a security policy, the participants stated thus:

Participant 3: *The critical assets should be identified and prioritised according to classes. The classes are measured with the value that these assets classes contribute to the core business of the department. Policy document is developed to support the primary mandate of the department.*

Participant 5: *The implemented security policy and plan. Senior level management support and buy-in.*

Participant 9: *It is the duty of the recruitment office to select the security manager that understands what the department seek to achieve. The vision and mission the department should be corner stone of every policy development. It is through threat assessment where the manager identifies the critical assets of the department and its vulnerabilities. The policy should be developed to improve the existing security measures and procedures. Security policy is a strategic plan to ensure that the core business of the department is not disrupted, and the critical assets are well protected.*

Participant 10: *The department security risk management policy should be in line with the state security agency policy. Positions within the departments should be graded according to access to classification of information as stated in the Miss documents.*

Participant 11: *Develop no-cell phones policy during sensitive meetings.*

Participant 12: *The programme directors who are part of the security committee identifies identify threats at their various units while members of SAPS and SSA plays an advisory role on the formulation of security policies. The security committee further makes* *recommendations to the HOD regarding the implementation and maintenance of security measures.*

Participant 30: *The process is to outline a broad policy statement that capture the broad goals and objectives of the organisation. The security risk assessment outlined above together with the business plan/ strategy of the organisation are valuable inputs in the formulation of a security policy that aligns to the core business.*

The above excerpts indicate that the department needs a security policy that deals with current security threats. The participants indicated that the Security directorate and the security committee should lead the process of coming up with the security policy that addresses each and every security threat. Brotby (2008: 27) reports that non-adherence to policy prescripts was a likely factor for poor service delivery and failure to reach departmental strategic objectives.

6.4.7.7 Training and Development

Security managers are responsible for conducting training needs assessment in order to identify the kind of security training that personnel should have (Brotby, 2008: 27). Most of the participants indicated that training and development is necessary as some members lacked the skills and knowledge to handle security information and tools. The participants indicated that the training may target security awareness, security when handling digital technologies and safety procedures for infrastructure. The participants echoed the following views:

Participant 4: *Training, test and exercise serve several purposes. They allow the security management team to use and assess plans and procedures to determine whether they are actually feasible and will work under actual conditions, assess and measure the degree to which personnel understand their emergency response function and duties, identify areas for improvement, enhance coordination, communication and proficiency among response staff and the ability of management and staff to respond to emergencies. Experienced gained and errors committed during exercises can provide valuable insights and lessons learned that can be included in the planning process.*

Participant 5 added: *Training shall be provided to enable employees to apply information technology security effectively and efficiently. Security consciousness shall continually be promoted amongst personnel and shall be followed up by means of formal training programmes where required.*

Participant 6: *Training and education to ensure reasonable levels of security awareness and preparedness within the business.*

The responses from participants indicated that training and development are necessary for the continued acquisition of knowledge of personnel. It is even kore important in an evolving techno, logically driven world. To that end, it is crucial for departmental employees to be aware of the security changes in order to safeguard the department against emerging threats (Maude, 2007). Some of the training involved fire drills. Normally, fire drill should be carried out every six months. However, in small buildings with few occupants and simple evaluation arrangements, annual fire drills might be acceptable, if justified by a fire risk assessment and provided the requirements of any fire certificate are satisfied.

6.4.7.8 Stakeholder Involvement

Evidently, most participants cited the vulnerability of departments to security threats. As such, there was an urgent need to introduce a security policy and security measures (Kabanda et al., 2010: 4). However, participants indicated that all these changes needed stakeholder involvement for them to be successful. The participants expressed that stakeholder for each security areas need to be consulted and participate in the policy development process. Following are the responses from participants:

Participant 9: *The Security Manager should involve all stakeholders from the beginning of the assessment. The core business of the department should be clearly defined, and the threat and risk picture should be clearly analysed. All business units should be involved to ensure that there is a budget to fund recommended security measures.*

Participant 10: *The SSA and SAPS are the main stakeholders to the department and should be consulted when developing the security policy and formulating the security committee.*

Participant 11: *Security Threat Assessment is a mandate of SAPS, and they are responsible for all physical security assessment and security breaches. The SSA is responsible security breaches relating to information and electronic communication issues.*

Participant 12: *Coming up with a security policy can be achieved by identifying and engaging with internal and external stakeholders. The relationship between the department and stakeholders should be maintained and monitored throughout the year.*

Participant 25: *The security managers should communicate the MISS documents to all stakeholders, employees, and service providers. All middle managers in the security component should have key performance indicators in their key performance area.*

The findings of the study point at stakeholder involvement as an important step towards the development of security policy and security strategies that are meant to mitigate the various security threats that have been discussed in this chapter.

6.4.7.9 The Key Role Players in the Public Service IT Risk/ Threat Environment

The following entities are the key role players in the public service IT risk environment.

a) The Department of Public Service and Administration (DPSA), whose mission it is to "ensure the effective use of information technology in government," "facilitate the use of information technology for modernizing government," and "establish e-government practices within an acceptable information security environment," is responsible for ensuring that information technology is used effectively in the government;

b) The Auditor General of South Africa (AG) audits Public Service IT risks related to Public Financial Management Act (PFMA) requirements;

c) The SSA is the leading authority on matters pertaining to state security, including Public Service IT risks. The SSA is also responsible for the system known as the Government Electronic Communications Security Computer Security Incident Response Team (ECS-CSIRT), which reports on critical security incidents pertaining to national security;

d) In its capacity as an excellence centre for the Public Service, the State IT Agency (SITA) has been charged with the responsibility of providing both a help desk service and information technology services that conform to the necessary safety standards. On the SITA helpdesk system (call log system), issues of the following sorts were reported: hosting services, managed apps, managed desktops, and network services; and

e) The Department of Telecommunications and Postal Services (DTPS) is responsible for formulating, coordinating, and providing policy direction on issues relating to information and communications technology (ICT). Additionally, DTPS will be responsible for the activities of the Cyber Security Hub and its objectives that are derived from the National Cybersecurity Policy Framework.

6.5 DISCUSSION OF SECURITY COMPONENT IN THE CONTEXT OF THE FINDINGS

The essentialisation of the security component emanates from the following important variables: security administration, physical security, the integration of physical security measures, information and communication technology (ICT) security, and internet access.

6.5.1 Security Administration

The functions of security administration include: General security administration (departmental directives and procedures, training, and awareness, security risk management, security audits, sharing of information and assets) (Cawthra, 2019: 223-224). Other functions include: setting access limitations, administering the screening of security screening, implementing physical security, ensuring protection of employees and information, ensuring ICT security, increasing and ensuring security in emergency and reducing threat situations, facilitating the BCP, ensuring contract security; as well as preventing security es by submitting reports and intensively investigating possible threats (Cawthra, 2019: 223-224).

6.5.2 Physical Security

The term "physical security" refers to, but is not limited to the following:

- Physical security measures for the protection of information;
- Personnel security awareness of physical security matters;
- Contingency planning;
- Criminal Record check;
- Dealing with security breaches relating to physical security matters;
- Security investigations;
- Auditing and compliance checks to ensure security standards.

In the context of this study, physical security refers to the arrangement and construction of the departments' facilities, as well as the implementation of various physical security measures, which are intended to both delay and prevent unwanted access to the departmental assets (Govender, 2018: 39). It involves the activation of appropriate responses upon the detection of real or attempted illegal access as well as the procedures necessary to detect such access. In addition, the provision of safeguards to protect personnel from bodily injury is included under the umbrella of physical security.

To guarantee the safety of the entire department, and its employees, assets, and information, it is necessary to design, put into action, and continue to maintain physical security measures (Mohlabeng, 2020: 3). The Head of Security's proposed TRA should serve as the basis for these security measures. The departments are responsible for ensuring that the process of planning, choosing, developing, and changing their facilities includes complete integration of physical security measures as early as possible. To that effect, the departments are required to undertake or perform the following tasks:

- Selection, designing, and modification of facilities to facilitate the effective control of access thereto;
- Demarcating restricted access areas and have the necessary entry barriers such as security systems, and effective control access of equipment;
- Inclusion of the necessary security specifications in planning, requesting of proposal and tender documents, and incorporating the related cost into funding requirements to implement the above; and
- Departments' responsibility to ensure the installation of necessary physical security measures in ensuring the secured storage, transmission, and disposal of classified and protected information in all of its forms.

All employees are always required to comply with access control procedures of departments. This includes producing ID cards upon entering any sites of departments, as well as the display thereof whilst on the premises and the escorting of official visitors.

6.5.3 The Integration of Physical Security Measures

The integration of physical security measures occurs in the early process of selecting, designing, or modifying facilities of the institution (Mohlabeng, 2020: 3). Such integration of security measures should entail:

- The selection, design, and modification of facilities in order to facilitate physical security measures;
- The demarcation and control of areas at the facilities;
- The installation of the necessary physical security equipment based on the assessments by SAPS-SAS; and
- The inclusion of the necessary security specifications for tender documentation process and the 23 Minimum Physical Security Standards (MPSS).

6.5.4 The Implementation of Physical Security Measures

The implementation of physical security measures is intended to fulfill the following:

- Activate appropriate reactions to such attempts or actual gaining of unlawful entry;
- Delay, detect, or prevent unauthorised infiltration into a department or institution;
- Delay, detect, or prevent unauthorised intrusion into a department or institution;
- The deployment of physical security measures to protect employees, visitors, and contractors from potential danger;
- The safe keeping, transit, and eventual disposal of the department's or institution's assets; and
- The ongoing examination of the department's or institution's physical security measures at all of its sites, in order to account for shifts in the external environment and make the most of innovative, cost-efficient technological advancements.

The afore-cited physical security measures cohere with the propositions by authors such as Chou (2013: 16), Garcia (2006: 14), Isnaini and Solikhatin (2020: 80, and John and White (2014: 12).

6.5.5 Information and Communication Technology (ICT) Security

It is required that a secure network be established for the departments in order to guarantee the protection of information systems against threats that are continuously evolving, and that may have an effect on the systems' ability to maintain their confidentiality, integrity, availability, and value in accordance with their intended use (Chou, 2013: 17). Baseline security controls and any extra measures that are found via the security TRA should be implemented by the departments in order to prevent the compromise of information technology systems.

These controls, as well as the duties and obligations regarding security that are held by all people, should be properly defined, recorded, and communicated to each and every individual working for the department (Chou, 2013: 17). In ensuring that policies are followed, the requirements for the Chief Technology Officer of each department to adhere to:

- Certification of all information technology (IT) systems and securing them after procurement;
- Accreditation of information technology (IT) systems prior to operation;
- To conduct periodic security evaluations of systems, which includes assessments of configuration changes to carry out on a routine basis;
- Periodic requesting of assistance, reviewing, and audits from the SSA in order to get an opinion on whether or not policies are being followed; and
- Ensuring that minimum security standards are in place.

Based on the above, it is then required that server rooms and any other relevant security zones that house IT equipment should be protected with suitable physical security measures, and that rigorous access control should be implemented and monitored (Chou, 2013: 17).

To avoid illegal use of the departments' network resources, access to such resources should be rigorously regulated and monitored. Unless otherwise specifically allowed access to all departmental computing and information systems and their peripherals ought to be strictly controlled (Fruhlinger, 2019: n.d). System hardware, operating and application software, as well as the network and communication systems of departments shall be configured and safeguarded against both physical attack and unauthorised network intrusion. This applies to both the network and communication systems as well as the network and application software. Every worker is required to utilise the information technology systems provided by the departments in an appropriate way and only for work-related reasons. Regarding this topic, each worker is required to always comply with the IT Security Directives.

Passwords are not to be disclosed to any other person, under any circumstances, for any purpose. Therefore, when choosing, using, and managing passwords as a mechanism to limit access to systems, there should be stringent adherence to best practice requirements, which are embodied in the IT Security Directives (Grama, 2011: 44). It is required that each department construct an information technology continuity plan as part of its overall BCP and recovery efforts. This will ensure that essential services are always available to users.

6.5.6 Internet Access

Internet access is the responsibility of the Chief Technology Officer of each department, who is also tasked with ensuring that the network of the departments is protected from malicious external intrusion by installing a configured firewall that as a bare minimum measure (Rishi, 2019: n.d.). The management team in charge of HR has to make certain that all employees who have access to the internet (including e-mail) are made aware of, and agree to abide by a reasonable code of behaviour regarding their use of the internet. It is also the core duty of the Chief Technology Officer of the Departments to control user access to the internet, as well as ensuring that users are informed of the dangers and safeguards in order to limit the risk of information security breaches and incidents (Rishi, 2019: n.d.). Due to the inherent hazards that email poses to information security, incoming email should be handled with the utmost care. Accordingly, it is forbidden to open e-mails that involve file attachments, unless those files have first been screened for any potential computer viruses or other forms of dangerous programming (Saleh, 2021: 85).

6.6 DEVELOPING/ DESIGNING AN EFFECTIVE AND IMPLEMENTABLE SECURITY THREAT ASSESSMENT MODEL OR FRAMEWORK

The development of an effective and implementable STA framework or model is in congruity with the final research objective as stated in Section 1.7 of this study, namely: *To develop/ design an effective and implementable security threat assessment model or framework.*

The above-stated objective is in correspondence with the final research question as stated in Section 1.8 of this study, namely: *Which possible solutions could be implemented to address the correct implementation of security threat assessment?*

Based on both the secondary data and primary data acquired in the study, it is recommended that the SSA should have a single STA methodology for government departments with different approaches based on the core business, but which align to the intended objectives and approaches.

6.6.1 Approach to STAF

The STAF approach should adhere to the following as proposed by Mills et al. (2011: 19) and Monzon (2021: 1).

- **Adaptability:** The new approach needs to be adaptable enough to manage all types of assets, including physical and information technology assets, as well as big and small assets, at a degree of detail that is appropriate to fulfil business objectives. It should enable several degrees of granularity with a roll-up capability, ranging from finely detailed or closely focused assessments to more general overviews, depending on the risk environment and the goal of the assessment;

- **Modularity:** The new technique has to facilitate modular analysis and have proper links between aspects that are connected to one another. This will enable the breakdown of bigger, more complicated STAs into smaller, more manageable components;
- **Ease of Application:** In order for programme and project managers, as well as security practitioners, to easily put this approach into practice, the underlying logic of the methodology should be intuitively pleasing and clearly expressed. To make the harmonized methodology more user-friendly, the key ideas and procedures of the methodology need to be comprehensively presented using a wide variety of charts, diagrams, examples, tables, and templates;
- **Consistency:** The new methodology ought to develop a consistent language with clear definitions for all elements of risk management in order to achieve better uniformity across STAs done by diverse agencies. This will allow for greater consistency in the results of the STAs. Comparative analysis and repeatable results are essential for informed risk communications, enhanced interoperability, and cost-effective security solutions. Solid risk variables measurements, especially asset valuations, threats, and vulnerabilities, are necessary for both of these;
- The technique should be relevant to both physical and information technology assets, in addition to employee protection and service delivery; and
- **Automation:** The STA Methodology is a manual tool, but it was built with automation in mind to assist simplify and support the STA process. This was done in order to meet the requirements of the Social Security Administration.

6.6.2 Security Threat Assessment Approaches

The security practitioners should understand the primary mandate of the departments and prioritisation of asset protection (Mills et al., 2011: 19; Monzon, 2021: 1).

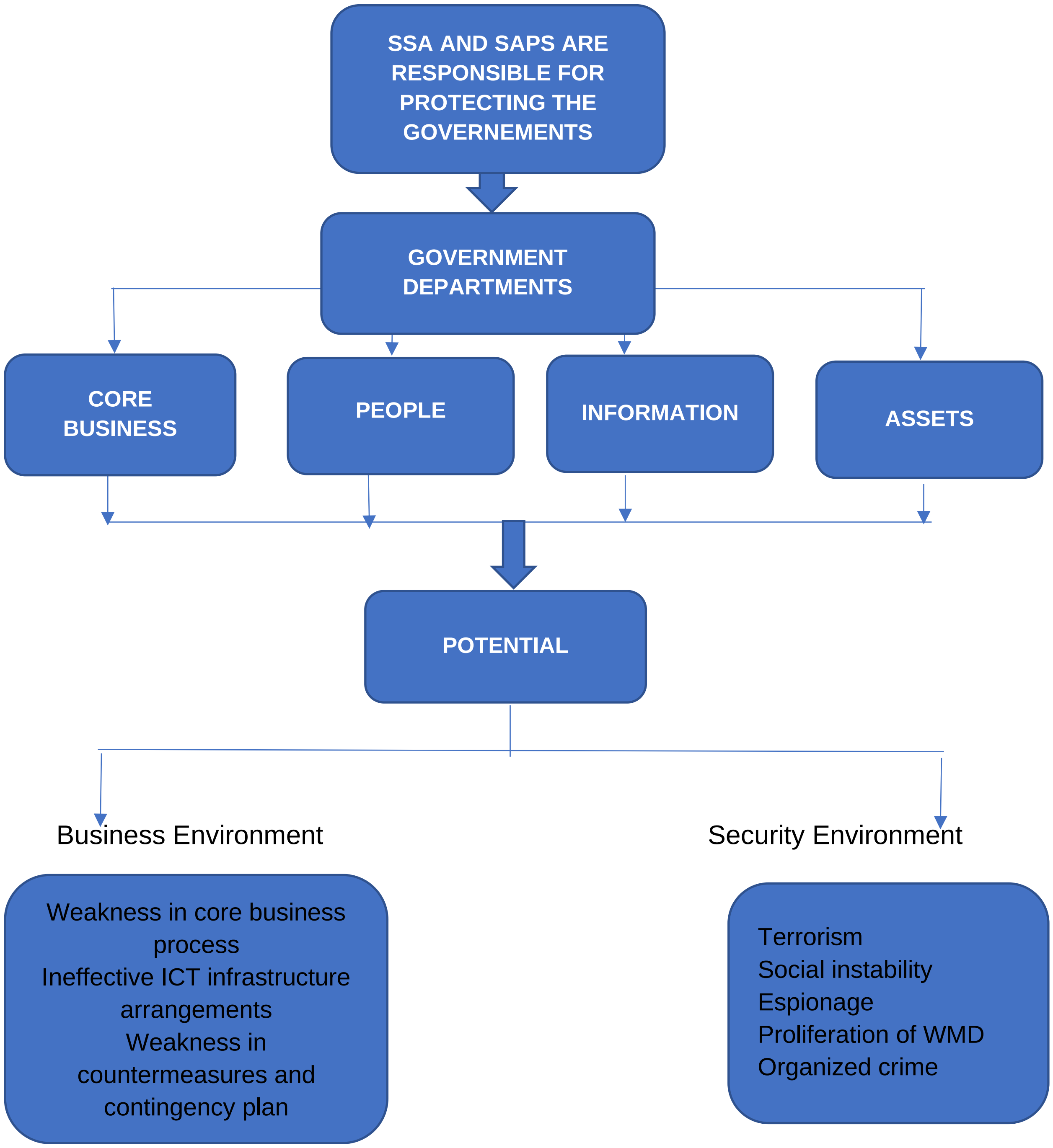
. The implementation of STA should be able to define the departments' threat picture and the vulnerabilities that should be addressed. It should be clear if the departments intend to:

1. Develop a strategy to secure facilities and critical infrastructure against acts of terrorism, insider threats, or natural catastrophes, and then implement that strategy;
2. Teach the security personnel how to recognise potentially dangerous persons, such as active shooters or terrorists, and provide them guidance on how to respond to them;
3. Identify, assess, and intervene with a person who may commit targeted or instrumental violence; or assess the overall likelihood that a specific individual for violent behaviour;
4. Protect the computer networks, systems, and servers from attacks by malicious actors;
5. Identify, assess, and intervene with a person who may commit targeted or instrumental violence; and
6. Assess the overall likelihood that a specific individual for violent behaviour.

This post is not meant to be a comprehensive review of each method. Rather, it is meant to define and help in identifying the need to implement the STA and what resources would be needed.

6.6.3 Proposed Threat and Risk Assessment Model

The micro-level institutional approach and framework for a threat and risk assessment model is illustrated in Figure 6.1 below.



SSA AND SAPS ARE RESPONSIBLE FOR PROTECTING THE GOVERNEMENTS
GOVERNMENT DEPARTMENTS
CORE BUSINESS
PEOPLE
INFORMATION
ASSETS
POTENTIAL
Business Environment
Security Environment
Weakness in core business process
Ineffective ICT infrastructure arrangements
Weakness in countermeasures and contingency plan
Terrorism
Social instability
Espionage
Proliferation of WMD
Organized crime

Figure 6.1: Framework for proposed threat and risk assessment model
Source: Researcher’s own proposal/ initiative

In more detail, the SSA’s approach to conducting STA entails the following:

- The core business process of the departments should be analysed and it existent should be careful explained and what does it do. It ought to be determined why is described as a national asset, and why it is seeking be protected. The process should include interpretation of the departments’ security policies and standards against the security vulnerabilities that has be identified.
- The threats against the departments should be analysed.
- Risks associated with each specific threat should be identified.
- The risk has to be assessed to determine the likelihood of threats happen, and their impact to the department and the government.
- According to SSA, the risk mitigation measures should formulate.

The STA is conducted by means of the following phases indicated in Table 6.4 below:

Table 6.2 Planning steps of STA

Planning	Planning and define the project – what will be assessed? Where will the assessment be conducted? What resources are needed?
Step 1	Analyse the departments’ core business and identify its key assets and relevant business processes to be protected.
Step 2	Identify and analyse all potential threats to the departments and define the specific risks that each of these threats could pose.
Step 3	Analyse the weaknesses and safeguards and identify exploitable vulnerabilities.
Step 4	Assess the identified risks, and compile a risk profile of the departments
Step 5	Recommend risk mitigation Strategies
Step 6	Monitor implementation and track compliance, and reassess residual risk

Source: Researcher’s compilation from various sources

The STA should be conducted at different stages of the departments' security programme development. Moreover, the STA ought to be reviewed as the development of progresses. The STA should also be reviewed on a regular basis and whenever circumstances change that could affect the risk level (Mbowe et al., 2014: 170; Saleh et al., 2011: 18). As a result, the STA should not be completed once and then forgotten. Figure 6.2 overleaf is a depiction of the STA’s code of conduct.

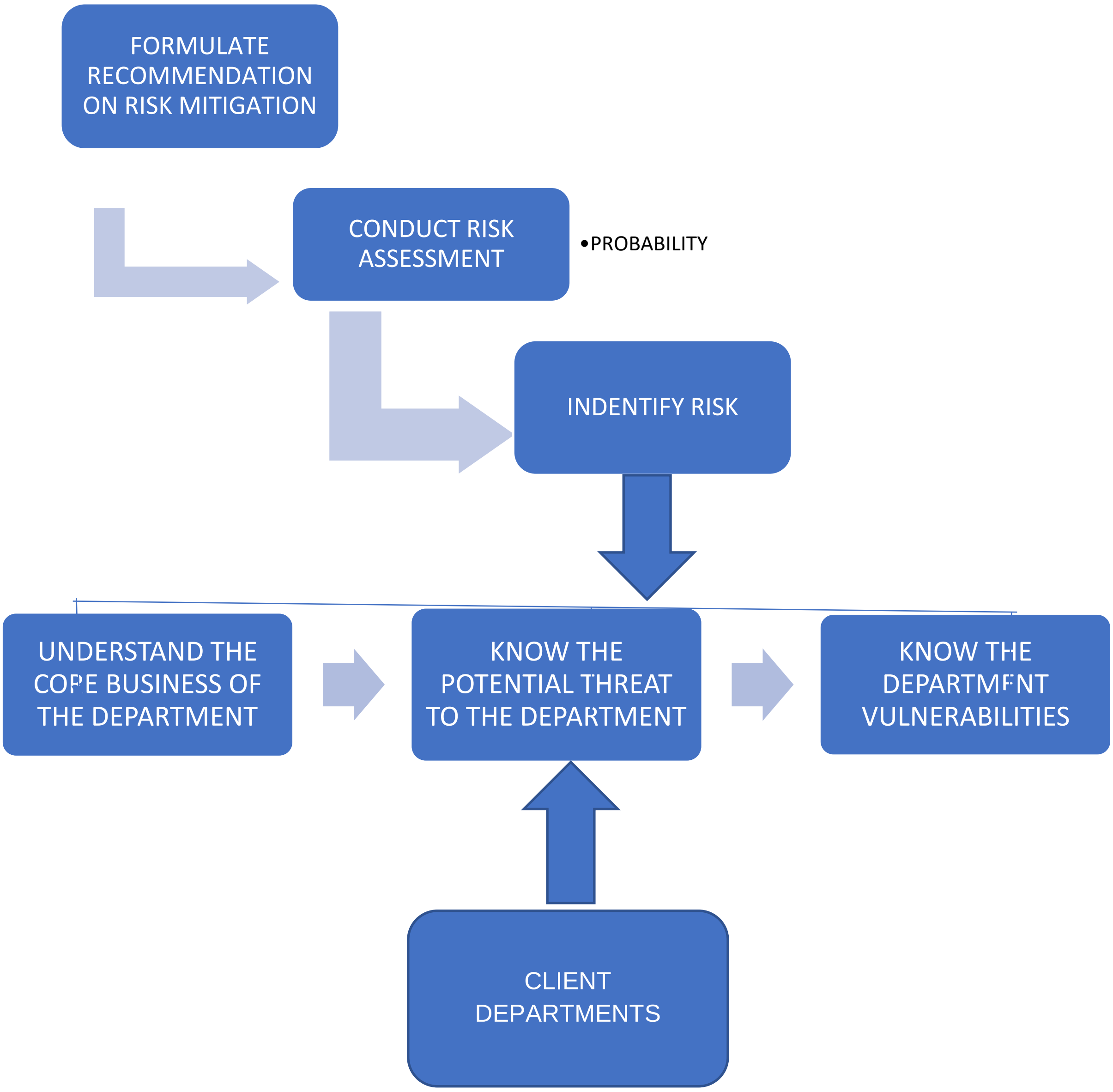

FORMULATE RECOMMENDATION ON RISK MITIGATION
CONDUCT RISK ASSESSMENT
•PROBABILITY
INDENTIFY RISK
UNDERSTAND THE CORE BUSINESS OF THE DEPARTMENT
KNOW THE POTENTIAL THREAT TO THE DEPARTMENT
KNOW THE DEPARTMENT VULNERABILITIES
CLIENT DEPARTMENTS

Figure 6.2: STA code of conduct
Source: Researcher's compilation

When the core business of the departments is clearly defined and the critical assets are identified, it is the responsibility of the HOD to appoint a security manager, who would compose the STA Team.

6.7 RECOMMENDATIONS

According to Tight (2017: 40) and Yin (2018: 109), recommendations are predominantly referred to as the researcher's own ideas intended for application to the study on account its findings. In essence, recommendations are a set or range of propositions by the researcher, and are intended for improvement in the various areas of research in which possible deficiencies were highlighted in the findings (Tight, 2017: 40; Yin, 2018: 109). Consistent with both the research aim, objectives and questions as articulated in Section 1.6 to Sections 1.8 respectively, the recommendations in this section fundamentally relate to:

- the scope of government's security threat assessment framework (STAF) guidelines;
- the role of other directorates when implementing the STAF;
- the role of management in supporting the security programmes;
- the processes for appointing the security manager and the security committee, and their respective roles in threat assessment;
- the departments' processes of anticipating and analysing the probabilities of loss and damage to State property;
- current layers of security measures; and
- possible solutions to be implemented in addressing the correct implementation of security threat assessment.

6.7.1 Recommendations Concerning the Scope of Government's Security Threat Assessment (STA) Framework Guidelines

The purpose of the assessment is frequently misunderstood at the outset of the project, which results in the failure of many STAs (Mbowe et al., 2014: 174). This always leads to lost work and avoidable delays, which is the reason for the need to specify the goal of the assessment, the amount of information that is required, and the constraints of the exercise right from the beginning. In general, the most successful STAs are those that are as concise as feasible while yet satisfying the requirement for making informed decisions. It is desirable to carry out multiple, smaller, more modular evaluations rather than one huge project in order to attain this goal, especially when dealing with larger projects or assets that are complicated. Naturally, changes can be made to accommodate the ever-evolving circumstances and the projects can be re-scoped when there is need, such as when the threats and vulnerabilities that were previously identified are discovered (Mbowe et al., 2014: 174).

The objective of conducting a STA is to:

- Analyse the core business of the departments and identify its critical assets;
- Identify how threat agents can compromise these critical and sensitive assets;
- Assess the level of risk that the threat agents pose to the critical and sensitive assets;
- Recommend risk mitigation Strategies; and
- Monitor implementation, track compliance and reassess residual risk.

The SSA uses the term "critical assets", which has also been used by the researcher to incorporate all the following classes: Core business processes; people; information; ICT assets; physical infrastructure; services; and intangible assets. This is also a definition adopted by Allen (2016: 18) and Kuzminykh et al. (2021: 605).

Table 6.3 below illustrates the interaction among these concepts to convey the implementation of STA.

Table 6.3: The interaction among these concepts to convey the implementation of STA

Example: Asset	Example Risk	Example: Threat
Core business process	• Loss of public confidence • Damage to the national interest • Inability to perform • Damage to buildings	Organised crime Corruption Terrorism
Personnel	• Loss of life • Damage to reputation • Loss of knowledge • Loss of skills • Loss of loyalty	Labour grievance Social instability Terrorism Espionage
Physical Infrastructure	• Damage to key equipment • Damage to buildings	Social instability Terrorism
ICT	• Loss of records • Loss of data integrity • Unauthorised access	Cyber attack Organised crime Espionage
Documents	• Unauthorised access	Organised crime

Source: Researcher's own illustration

6.7.2 Recommendations Concerning the Role of Other Directorates when Implementing the STAF

Essentially, the role and responsibilities of national government departments entail the following:

- Ensure that the requirements of physical security directives relating to contracting are fulfilled with when the National Department of is responsible for providing facilities for institutions. These directives are related to physical security;
- Make sure that the necessary National Intelligence Structures of private organisations, corporations, and individuals who could need access to protected and classified information and assets carry out dependability checks on each other before allowing them access to the information or assets in question;
- As part of the contracting procedure, make sure that the department or institution adheres to the physical security measures that have been specified by the SAPS Security Advisory Services for the installations of the department or institution;
- Ensure that security assessments of facilities or drawings/architectural designs thereof are carried out by the SAPS and SSA prior to any agreement being entered into to procure the property for an institution, and that all recommendations made by the SAPS are implemented. This should take place before any agreement is entered into to procure the property for an institution; and
- Include the SAPS in any and all structural modifications undertaken to ensure that the required degree of basic physical security is maintained at the departments.

Based on the findings regarding Research Question 2, the contextualisation of the role of other directorates when implementing the STAF is premised on the following variables: human resources security; communications and operations; ICT risk assessment; and asset management.

6.4.2.2.1 Human resource security

Human resource security aims at ensuring that all employees and applicants to the departments are appropriately security vetted and meet all the requirements to handle information and technology security, and they acquire knowledge on how to implement their responsibilities relating to security (Singh, 2019: 2013). To reduce security risks, they should keep in mind relevant prescripts such as laws, regulations, and policies, business requirements, information classification to be accessed, and perceived risks, including those posed by technology, throughout the entire employment/ contracting cycle, from recruitment to termination of employment.

Their security-related role and responsibilities should be clearly stated in their employment contract. Whilst employed, it is the responsibility of security management to ensure that all guidelines related to security are adhered to. The security clearance process can be time-consuming, and while employees are performing their duties, management should ensure that they sign a declaration of secrecy as an agreement to ensure that official information is not disclosed to unauthorised people (Smith, 2019: 188).

Before employment, throughout employment, and after employment has ended, management and personnel are each subject to a unique set of security obligations and liabilities (Campbell-Young, 2016: 12). Prior to hiring, the focus is placed on gaining a knowledge of the tasks and responsibilities that will be required of the individual, screening prospects, and establishing agreements. In addition, policies should specify management duties, education and training requirements, and formal mechanisms to deal with potentially dangerous security circumstances that may arise while an employee is on the job (Campbell-Young, 2016: 12). It is important to set regulations in order to facilitate a seamless transition in the event that an employee's or contractor's employment or contract is terminated or otherwise altered.

6.4.2.2.2 Communications and operations

The purpose of communications and operations management security is to protect data within networks and guarantee the correct and safe operation of information processing facilities that support communications and operations (Kuzminykh &

Carlsson, 2018: 52). Therefore, it is necessary to plan and manage day-to-day operations in order to guarantee the availability of resources and the capacity of those resources to perform services. It is possible for a variety of services to be provided, by third parties, computer networks, and any and all services that share information (Kuzminykh & Carlsson, 2018: 52).

It is necessary to identify the specifications for regulating and monitoring the operations involved in the supply of services, and it is also necessary to manage changes as the operations develop. Changes that are made to departments, business processes, information processing facilities, or information storage and retrieval systems that might compromise information security should be controlled (Government of Canada, 2016). It is imperative that the integrity of operational systems be protected at all costs, and that technical vulnerabilities be circumvented. Controls for operations consist of defined procedures, assigned duties for staff, and formalized means for putting into action modifications to the facility. This covers processes for the protection of data, the generation of backup copies, and the administration of the media on which those copies are stored (Lohrmann, 2021: 16).

The installation of software by users ought to be controlled. The management and control of networks ought to be carried out by means of service agreements, regardless of whether or not network services are carried out internally or contracted out. This is done to ensure the security of electronic data (Lohrmann, 2021: 16). It is imperative that the confidentiality of all information transfers, whether they take place internally or externally, be preserved across all channels of communication, and that this information be safeguarded in line with the expected degree of safety.

6.4.2.2.3 ICT Risk management

The STA is used to determine how well the department's data are protected. In order to protect all of the many kinds of information that are housed or used by the departments, it is necessary to implement risk management procedures (Mandell, 2013: 17). These procedures ought to take into account the dangers posed by technical, human, and physical hazards.

The departments ought to have a methodology and process in place for ICT risk management in order to implement management policies, procedures, practices, communication, consultation, establishing the context, identifying the risk owner(s) who are accountable and have the authority to manage the risk, developing risk criteria, identifying, analysing, evaluating, treating, monitoring, and reviewing risk in order to determine whether the risk and/or its magnitude is acceptable (Mandell, 2013: 17).

The departments ought to make certain that the information and communications technology risks are managed within the context of the internal risk management practice in accordance with the risk management prescripts, and that the information and communications technology security function is audited as a component of the audit plan for the departments (Allen, 2016: 24).

During risk assessments for ICT security, the risks should be identified, quantified, and prioritised based on risk acceptance criteria and department-specific goals. The results should be used to define the appropriate management action and priorities for managing information security risks and putting in place controls that have been selected to reduce these risks (Amundrud et al., 2017: 4). It is advised that the department use the following methods and processes in order to institutionalise adequate information and communication technology security risk management:

a) Management system, and then allocate roles, duties, and accountability;
b) Install the necessary information and communication technology security risk;
c) Construct an exhaustive ICT security risk management methodology;
d) Put into action an ICT security risk management programme based on corporate goals and objectives;
e) Put into action the risk assessment procedure;
f) Conduct comprehensive risk assessments to identify, analyse, and evaluate related risks e) Choose proportionate ICT security controls as needed to reduce risk to an acceptable level;
g) Create risk criteria against which the significance of risk is assessed;
h) Choose proportionate ICT security controls as needed to reduce risk to an acceptable level g) Choose proportionate ICT security controls as needed to reduce risk to an acceptable level;
i) The risks should be analysed by comparing the findings of risk analysis with risk criteria in order to establish if the risk and/or the level of the risk are acceptable or bearable; risks should be continually monitored, and remedial action should be done, as necessary;
j) Institutions should develop and maintain ICT risk registers (Strategic and operational ICT risk register); and
k) ICT risks should be included in the institution's risk registers and monitored as the rest of the institution's risks. Risk avoidance is different from risk management.

The strategy that is used need to have justification in addition to being open to scrutiny. The concepts of risk management should be incorporated into day-to-day operations, and security concerns should be assessed and reassessed on a regular basis (Watts, 2017: 13). The tactics used by institutions have to be malleable and, in a position to react quickly to fast-moving or unexpected occurrences.

6.4.2.2.4 Asset management

Information and the many technologies used to store and retrieve it are vital government resources. Asset management should identify the parameters for the appropriate use of information, technological, and infrastructure assets, as well as the protection of such parameters (Watts, 2017: 13). In order to keep the security intact, roles and responsibilities need to be delegated, relevant asset management processes and systems need to be developed and kept up to date, asset inventories need to be developed and kept up to date, and acceptable and unacceptable uses of assets need to be defined (Rosencrance. 2022: n.d.).

It is necessary to determine who the authorised owners of assets are. The owners of information and technological assets are responsible for ensuring their safety (Rosencrance. 2022: n.d.). The information owners are tasked with determining the assets that need to be safeguarded, classifying the various security levels of the various assets, defining the sufficient protection that is necessary at each level, and determining how the protection will be maintained.

6.7.3 Recommendations Concerning the Role of Management in Supporting Security Programmes

The lack of management support in providing resources and capacity to effectively implement the STA shows that the national security is not a priority. According to Govender (2018: 12), for security managers to gain approval and support from the senior management, they should first understand the core business of the departments, be able to define the role of security clearly, and know when the departments are facing threats and risks. Senior management is very influential and an important component for a successful implementation of security programme (Whitman & Mattord, 2015: 34).

The management of the departments, employees and partner departments form part of stakeholders, and have potential to have negative impact to the departments, but they can also have a positive impact in mitigating the risk and threats. Their inputs to risk management are vital and they ought to be completely included in the process (Watt, 2017: 6). Campbell-Young (2016: 20) concurs with Watt (2017: 6) that the management need to be aware that if a major security incident happens, and it is published in the media, the management of the department will still the headlines.

Campbell-Young (2016: 20) adds that the management, in particular the Corporate Finance Officer, are now participating in addressing security and governance issues, instead on putting the whole responsibility of the experts.

As their first major responsibility, the TRA team should produce a detailed work plan in order to guarantee a coordinated effort that satisfies the operational demands of programme managers and departmental executives (Sahoo, 2021: 27). This strategy ought to be approved by the risk acceptance authority, which will finally go through the suggestions and decide whether or not to accept or reject the anticipated residual risk reported in the TRA report (Sahoo, 2021: 27). The precise amount of detail will differ depending on the breadth and scale of the evaluation; nonetheless, the plan should at a bare minimum include the following information:

The mission, purpose, scope, and terms of reference that have been created for the TRA:

- The core team and any other resources that are available to them, together with brief terms of reference for each; and
- Project inputs that are pertinent, including but not limited to past TRA data, privacy impact assessments (PIAs), business impact analyses (BIAs), design paperwork, facility floor plans, and so on.

6.7.4 Recommendations Concerning the Process of Appointing the Security Manager and the Security Committee, and their Respective Roles in Threat Assessment

It is the responsibility of the head of the departments to establish a security committee and appoint qualified security manager in an appropriate level, to oversee the implementation of STA (Sotic et al., 2014: 48). The security manager shall automatically become chairperson of the security committee. The security committee should at least have one representative from each chief directorate HOD, as well as one from each of the following components: Member of the Ministerial Office, HOD Office, HRM, Assets Management or Records Management, Risk, and ICT (DPSA, 2016: 11).

Furthermore, members and their proxies shall be appointed by virtue of their employment and ranks by the departments as well as their ranks and not as individuals (DPSA, 2016: 11). External members shall be considered as well, provided that they are in possession of a valid security clearance. In the absence of a proper clearance, certificate declaration of secrecy needs to be signed prior to commencement of the meeting.

6.7.4.1 Head of Departments

The HOD bears the overall responsibility for implementing and enforcing the security programme of the departments, and has delegated the function of security to the Head of Security (DPSA, 2016: 11; Sotic et al., 2014: 48). Towards the execution of this responsibility, the Head of Public Safety shall:

- Create the position of Head of Security and select a security official who is well-trained, knowledgeable, and competent in order to guarantee that all security duties are carried out in accordance with the Minimum Physical Security Standards;
- Create a security committee for the institution, make sure that all senior staff members participate in it, and approve a budget based on the committee's recommendations for the suggestions on the security assessment that was carried out by the SAPS (SAS) in the department/institution;
- Participation of management members from all the core business functions of the departments in the activities of the committee;
- Approval of this policy and all of its associated Security Directives, as well as compliance with these policies by all personnel and entities to which it is applicable;
- Be responsible for overseeing the formulation, execution, and upkeep of the security policy in accordance with the requirements of the department or institution; and
- Ensure that the SAPS Security Advisory Services have performed security evaluations and assessments on all of the departments that fall within his or her purview.

6.7.4.2 Security Committee

Participation in the activities of the Security Committee by the designated representatives of business units shall be required of them in order for them to be considered valid. The Security Committee is comprised of senior managers of the department who are responsible for representing all of the primary business units (Sutton, 2015). Assist the Head of Security in the execution of all security related responsibilities within the departments, including completing tasks such as drafting/reviewing of the Security Policy and plan, conducting of a security Threat and Risk Assessment, conducting security audits, drafting a BCP, and assisting with security awareness and training. The Security Committee of the departments shall be responsible for, among others, the following: Assist the Head of Security in the execution of all security related responsibilities.

6.7.4.2.1 Responsibilities of the security committee

a) Assist SM in developing the department's security policy after consulting with the SSA and the SAPS and considering their advice;

b) Assist in ongoing assessments of the institution's security threats, risks, and vulnerabilities;

c) Analyse all information obtained to determine the threats and vulnerabilities of information and assets requiring the protection;
d) Evaluate the probability of such threats materializing and vulnerability being exploited and the probable impact or severity thereof;
e) Make recommendations to the HOD regarding the implementation and maintenance of defensive counter-intelligence measures above baseline levels that will reduce risk to an acceptable level;
f) Regularly review the department's security policy, considering the risks identified by the committee, its prioritization thereof, as well as information and advice provided by the SSA and the SAPS;
g) Ensure that the approved policy is communicated to all staff members, relevant consultants, contractors, and other stakeholders; and
h) Make recommendations to the HOD on directives to be issued by him/her to ensure the implementation of the security policy and any review thereof.

6.7.4.2.2 Head of security (security manager)

Establishing and directing a security programme that assures the coordination of all policy functions and the implementation of policy requirements will be delegated to the Security Manager (Head of Security) by the HOD, who will transfer the role of security to the Security Manager (Fay & Patterson, 2018: 4). Due to the importance of this role, a Head of Security should be appointed. This Head of Security will have sufficient experience and training in the field of security and will be strategically positioned within the departments in order to provide senior management with institution-wide strategic advice and guidance (Fay & Patterson, 2018: 4). It is the responsibility of the Security Manager to make certain that the Head of Security is provided with an efficient support structure (security component) so that they can carry out their tasks.

The individuals who will be employed in the support structure of the Head of Security **should** be security professionals who have obtained sufficient experience and training in the field of security in order to properly perform the duties associated with their particular jobs (Cawthra, 2019: 223). The head of the security component should have direct access to the head of the institution and/ or a seat in management meetings addressing functional matters and policy in order to guarantee that information security is carried out on a sound basis throughout the whole organisation. In the wake of it, "Security" should be elevated to the status of a standing item on the agenda.

The Head of Security of each department is responsible for the implementation of the whole security function and programme inside departments (Dhillon, 2006: Fay & Patterson, 2018: 3-4). This obligation falls under the purview of the Head of Security of each department (coordination, planning, implementation, and control). In order to fulfil his/ her duties, the Head of Security is responsible for, amongst other functions:

- Serving as the chairperson or co-chairperson of the security committee alongside the individual who is nominated by the office of the Head of Public Safety;
- Working in concert with the security committee, draft the internal Security Policy as well as the Security Plan for the departments, which should include the thorough and precise Security Directives;
- Regularly reviewing the Security Policy and the Security Plan;
- Carrying out an analysis of the potential dangers posed by each department's operations with the help of the security committee;
- Conducting internal compliance audits and inspections at the departments at regular intervals;
- Liaising with SSA, SAPS, PSIRA, and other law enforcement agencies;
- Advising management on the security implications of management decisions;
- Putting in place a security awareness programme;
- •Implementing a security awareness programme; and
- Advising management on the security implications of management decisions.

6.7.5 Recommendations Concerning Government Departments' Processes of Anticipating and Analysing the Probabilities of Loss and Damage to State Property

Loss and damage are significant on a number of different levels. First, the methods of assessing loss and damage to state property offer a way to determine the extent of the devastation caused by a disaster to a natural environment or to the facilities of a department that could be affected by the event (Yamagata-Lynch, 2010: 12). In light of this, anticipating and analysing the probabilities of loss and damage to property should strive to achieve a conclusion that is more differentiated, complete, and centred on the needs of personnel and clients rather than only a basic stocktaking of impacts. Therefore, evaluations of loss and damage appropriately reflect a post-disaster reality. This gives impacted populations acknowledgement of their plight and provides a solid basis for strategies to prevent, mitigate, and address loss and damage in the future. Additionally, by doing so, it offers important input for adaptation efforts to be made to more sophisticated criminals.

6.7.5.1 Personnel Security Vetting

To obtain a security clearance at the appropriate level, all department employees, contractors, and consultants who are required to have access to classified information and critical assets to perform their duties or functions are required to go through a vetting investigation that is carried out by the SSA (Rishi, 2019: n.d.). If they pass this investigation, they will be granted a security clearance. The level of security clearance that will be granted to a person is based on the nature of the classified information that person will be required to access because of the post that he/she currently holds or will hold in the future in accordance with their respective responsibilities and accountability (Renfroe & Smith, 2016: n.d.).

Access to classified material that is governed by the “need-to-know” principle is made possible by having a security clearance. As part of the comprehensive process of screening for security risks, each person who is granted a security clearance should first sign a declaration affirming their commitment to maintaining confidentiality. This will continue to be true even after the individual in question has completed the duties associated with Departments (Smith & Brooks, 2013: 26). For a period of 10 years, a security clearance will be valid for the confidential level, and for a period of five years, it will be valid for the secret and top-secret levels. This does not prohibit the possibility of re-screening on a more frequent basis, as defined by the Heads of Departments, on the basis of information that has a detrimental influence on an individual's security competence. It is immediately required that security clearances be revoked for any and all employees whose employment with departments has come to an end.

6.7.5.2 Polygraph Examination

A polygraph examination is carried out on each potential candidate in order to supplement security screening (Bishop, 2003, 68). With the employee's prior approval in writing, a polygraph test will be administered to every worker who is required to undergo the Top-Secret security clearance process. The applicant is not viewed as suspicious or at risk in any way, shape, or form because of their participation in the polygraph screening process; rather, its sole purpose is to evaluate the accuracy of the information obtained throughout the security screening investigation. In the event that any unfavourable information regarding the applicant is obtained during the security vetting investigation (at any level), the applicant will be given the opportunity to demonstrate his or her honesty and/or innocence by participating in a polygraph examination (Fay & Patterson, 2018: 17). This opportunity will be provided in the event that any unfavourable information is obtained. The applicant's refusal to undergo the examination does not necessarily mean that a security clearance will not be given. However, it does increase the likelihood of this outcome.

6.7.5.3 Transferability of Security Clearances

It is not acceptable for a security clearance that has been granted to an official by one of the other government institutions to be automatically transferred to another department (Defence Science and Technology Organisation. 2010). The HOD is the person responsible for deciding whether or not the official should undergo further screening.

6.7.5.4 Security Awareness and Training

For the purpose of successfully ensuring that all people and service providers of departments continue to be security conscious, the Head of Security should establish and implement a security training and awareness programme as proposed by the DPSA (2016: 13). Every worker is required to go through the mandatory security awareness and training programmes, after which they should sign a document stating that they have read, comprehended, and agree to abide by the rules outlined in the programmes. The programme educates employees, relevant contractors and consultants about the security policy and security measures of departments as well as the need to protect sensitive information against disclosure, loss, or destruction.

Additionally, the programme provides training in regard to specific security responsibilities. In order to improve the training and awareness programme, regular security awareness presentations, briefings, and workshops will be held, and posters and pamphlets will be disseminated on a regular basis (DPSA, 2016: 13). All workers who have been recognised and advised that they are expected to attend the events are required to attend the programmes that have been outlined above. In order to monitor how successfully the security training and awareness programme is being implemented, the Head of Security along with other members of the security component are required to undertake routine surveys and walkthrough inspections.

6.7.5.6 Security Incident/ Breaches Reporting Process

When an employee of the departments becomes aware of an incident that might constitute a security breach or an unauthorised disclosure of information (whether accidentally or intentionally), they are obligated to report it to the Head of Security of the departments by making use of the formal reporting procedure that is prescribed in the security breach directives of the departments. This has to be undertaken in order for the incident to be properly investigated (Moagi, 2009).

Every instance of a security breach, whether confirmed or suspected, is to be reported by the Security Manager to the relevant authority (as specified in the Security Breach Directives of the departments), so that an investigation can be conducted (Monzon, 2021). It is the responsibility of the Head of Security of each department to ensure that the processes for reporting breaches in security are communicated to all of the workers. To handle any and all security breaches or suspected breaches that are reported, the Head of Security is obligated to design and put into action a response process for security breaches across all of the departments.

The individual in charge of security is responsible for seeing to it that the individual in charge of public safety is informed of any events of this kind as quickly as feasible. The SSA and the SAPS are tasked with conducting investigations into any suspected breaches of security and providing feedback along with recommendations to the relevant departments (Pinnock, 2020). As a result of investigations into security breaches or alleged security breaches, the HOD has the authority to suspend access rights to classified information, assets, and/or premises until the administration, disciplinary, and/or criminal proceedings have been completed. When deciding whether or not to restore, limit, or revoke an individual's security access privileges, or whether or not to revoke or alter the individual's security clearance, the HOD may take into consideration the results of these investigations, disciplinary action, or criminal prosecutions. In addition, the HOD may decide whether or not to alter the individual's security clearance.

6.7.6 Recommendations Concerning Capacity and Adequacy of Current Layers of Security Measures to Prevent Threats Before They Occur

Based on both the secondary data and primary data accrued in the study, the prevalence of a viable security policy in departments is viewed as a conducive proposition for enhancing strategies and mechanisms to prevent threats before they occur. In that regard. Table 6.4 overleaf expounds on the tactical measures for such prevention and strengthening of the capacity of departments.

Table 6.4: Description and examples of tactical measures

Strategy	Description and examples of tactical measures
Confront	The decision-makers concludes that the risk should be addressed because of the seriousness of its anticipated impact, the high possibility of its occurrence, and the timeliness of its occurrence. A decision to go with this alternative requires not only the availability of sufficient resources to support any countermeasures, but also the political will to implement drastic countermeasures, as well as a strong belief that the anticipated positive long-term results would eventually outweigh inevitable negative ramifications in the interim period. Common strategies that should be taken into consideration include legal prosecutions, the introduction of new legislation, the issuing of ban orders to departments, the arrest of prominent leaders, confrontations of a military nature, public exposure of foreign agents, and other similar strategies.
Reduce	The policymakers conclude that the risk, even if it is considered to be serious, cannot be effectively confronted due to the absence of sufficient resources; the unacceptable cost of potential negative ramifications; or the absence of the political will to introduce drastic countermeasures. Instead, the focus is being placed on playing down the seriousness of the risk (e.g., from high to low risk). The deployment of security forces, the conduct of strategic political intervention, the conduct of talks, and the upgrading of the physical security of sensitive locations are all examples of typical ME techniques that should be considered.
Contain	This is at best an interim plan, and its goal is to mitigate the negative impacts of a risk in the short term in order to stall until a strategy that is more all-encompassing can be chosen and implemented. It would often be used as an emergency measure in situations in which unexpected risks unexpectedly appear without any warning, and it would typically comprise a mixture of confrontational and reduction approaches, all of which would be carried out under the guidance of contingency planning.
Avoid	The decision-maker in charge of policy concludes that the danger is extremely unlikely to materialize in the short to medium term, but that it is unavoidable in the longer term. Options that involve confrontation or a downgrade in status are not considered to be viable. As a result, the decision-maker concludes that the only way to steer clear of the risk in its entirety is to make changes to a previously held future vision that are both strategic and preventative in nature.
Carry	The decision-maker is fully aware of the repercussions of the risk, but he or she nevertheless concludes that it is worthwhile to take the risk and that the risk associated with the risk's continuous presence is offset by the prospect of a bigger opportunity being taken advantage of. A common illustration of this would be the situation in which operations of foreign intelligence are discovered but are permitted to continue since it is believed that they could lead to the discovery of a larger network.

Source: Researcher’s compilation from various sources

6.7.6.1 Implementable Security Policy Architecture

A Security policy is a general declaration of intent that gives direction on what position security plays inside the department (Turianskyi, 2018: 14). Security policy can be classified as a combination of system-specific, issue-specific, and organisational policy, and should be used to:

- Identify the departments' most valued assets;
- Departments' vision in relate to security;
- Summarise the roles of personnel within the department;
- Describe the role of directorate security within the department;
- Outline the departments' contingency plan; and
- Outline the departments' legalities in relate to standard operation procedure.

The Security Manager is responsible for coordination and execution of the STA to clearly define the departments' threat picture and understand the weaknesses in the existing security measures. When threat and risk sources are clearly defined, the critical assets withing the core business of the department can be clearly identified (Vellani, 2020). The Security Manager should use the intelligence gathered to contribute to the development and communicating of the draft document to the Security Committee. The draft documents for consideration by the Security Committee will be submitted in the normal course at least four working days prior to the meeting date. This will enable the members to study the documentation and allow adequate opportunity for both formal and informal discussions.

Each member should be allowed to play a full and constructive role in the affairs of the Security committee and shall be furnished with all relevant information/details before making any decision. Members shall conduct themselves in a befitting manner and show respect to one another. Decisions taken by the Committee are binding and can only be changed by the HOD.

- Which are the departments' processes of anticipating and analysing the probabilities of loss and damage to State property?
- What are current layers of security measures?
- What solutions should be implemented to address the correct implementation of security threat assessment?

The security policy covers the following seven elements of the security programme of the department:

- Security organisation;
- Security administration;
- Information security;

- Physical security;
- Personnel security;
- ICT security; and
- BCP.

The security policy should include protection of the following:

- Confidentiality: Ensuring that information and systems are accessible only to authorised users;
- Integrity: Safeguarding the accuracy and completeness of information processing methods; and
- Availability: Ensuring that authorised users have access to information and systems when required

6.7.6.2 Requirements for a Security Policy

The proposed security policy should entail the following:

- It should be a clearly defined document that encompasses the Minimum Physical Security Standards;
- It should cover all aspects of physical security and provide for different levels of physical security grading;
- It should set out the obligations of the different role players about the implementation of the policy;
- The policy should clearly give a direct guide to all personnel and relevant contractors and consultants of the department/institution to adhere / comply with the Minimum Physical Security Standards;
- The policy should clearly specify that failure by an employee to comply with the policy and the Minimum Physical Security Standards constitutes serious misconduct and those disciplinary measures should be taken against such a person; and
- Security Manager should develop operating standards to ensure that they achieve operational objectives.

In order to successfully execute the STA, security managers need to place a key emphasis not only on the core and legislative responsibilities of the department, but also on the efficiency of the physical security measures currently in place and information security (Troy, 2020: 17). If the legislative mission of the department is understood and well-known, the security component of the department will be able to detect potential security risks that may affect the department. After a threat or risk has been discovered, a risk mitigation strategy can be effectively put into place to eliminate or avoid the threat or risk, as well as any potential hazards that have been identified.

The creation of security rules and procedures occurs once the STA has been effectively implemented (Vellani, 2020). Before the HOD gives his or her blessing, check to see that the backing of the security policy comes from the labour unions. The security policy and procedures should cover not only the physical security measures but also the information security measures, the information technology security measures, the communication security measures, the personnel security vetting measures, and the personnel suitability checks (screening) measures.

After consulting with all of the stakeholders and the security committee, the security manager should make sure that the policy is written in accordance with the guidelines provided by the MISS document, and that it refers to other policies, procedures, and plans that are related to the primary mandate of the department (South Africa, 2017). This should be done after ensuring that the policy is written in accordance with the guidelines provided by National Legislation. Following the completion of all of the consultations, the draft policy will be sent to the SSA for their consideration and approval. After the SSA has provided its approval of the draft policy, it should then sent to the head of the department for final approval (South Africa, 2017). After receiving approval from the HOD, the policy will then be disseminated to all of the departments' business units, as well as contractors and other stakeholders, through awareness programmes, an intranet internal website, and by making it accessible to all workers. Subsequently, the security policy would then be put into effect.

6.8 VALUE/ CONTRIBUTION OF THE STUDY

The results of the research will contribute towards bridging the gap between well-developed security frameworks on the one hand, and a lack of implementation in South African government departments, on the other (Wagner et al., 2012; Yin, 2018: 11-12). The findings have revealed the nature and scope of issues encountered by security personnel responsible for implementing the security threat assessment and other risk control procedures. The research shows that departments that adhere to the methods outlined in this thesis, performed effective security threat assessment and saw considerable reductions in vulnerabilities. In that regard, this study and its results contribute to new knowledge and builds excellent practices to give effective and implementable guidelines and procedures for the STA at all levels of government. Furthermore, the information gathered from this study will help security professionals and senior management understand their critical role in supporting security policies and procedures.

The research emphasises the need of understanding the departments' core business in order to identify critical asserts that seek to be protected. This will add value to security management and security committees, including the development of policies and standard operating procedures are developed, as well as appointment of skilled security managers. The findings reveal further that executive management should be actively involved in assessing emerging threats and providing effective security risk control procedures in order to improve current protection mechanism and charting new avenues for research.

It is envisaged that the study will contribute meaningfully to learners who are studying towards security-related qualifications, as well as to the academic community once the research has been disseminated through the University of South Africa’s internet library system.

6.9 POSSIBLE LIMITATIONS OF THE STUDY

Although generalisability is not necessarily the particular focus of qualitative studies (Anderson & Poole, 2014: 13; Gupta & Awasthy, 2015: 28), the current study’s findings could possibly be limited by the non-involvement of more security stakeholders in other national governmental departments. However, there were key government departments in Gauteng Province that were reluctant to participate in the research, which impacted on the possible generalisability of the findings and therefore reflect a limitation of the research.

6.10 CONCLUSION

Threat assessment represents one part of a comprehensive approach to prevention and securing the safety of government departments, to positively assist the personnel and clients, where a good platform is created to report matters concerning security of the people, assets, and information. Because it is in South Africa's national interest to protect its departments, the SSA is legally mandated to gather, collate, and analyse intelligence, as well as provide advice and vetting services, to protect these departments from threats to national security. Terrorism, espionage, the proliferation of weapons of mass destruction, organised crime, and social instability are examples of such threats, as they are threats arising from inherent vulnerabilities within these departments. vulnerabilities in their physical security arrangements, personnel security, information technology security, or the integrity of their business processes.

Government departments retain independent responsibility for managing security and non-security related business threats and vulnerabilities. If these vulnerabilities and threats are likely to have an impact on the national interest, and thus on national security, they fall under the SSA's offensive and defensive mandate. All these departments have their specific valuable assets that should be safeguarded for national security reasons. These areas are commonly referred to as the department's key assets, and they include its personnel, information, IT, and communication systems, as well as the department's reputation and ability to perform those critical business functions for South Africa's national interest and national security.

REFERENCES

Abedian, I. 2004. Balancing the nation's books: in Parsons, R., Abedian, I., DuToit, P., Dykes, D., Friedman, S., Kantor, B., Mnyanda, L., Roux, A & Steyn, G. *Manual*, *markets and money double story books*, Cape Town: Juta.

Accenture. 2019. *Insight into the cyber landscape in South Africa*. Available from: https://www.accenture.com/_acnmedia/PDF-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf (Accessed: 18 February 2022).

Adams, W. 2015. *Handbook of practical program evaluation*: *Conducting semi-structured interviews.* Washington, D.C: George Washington University

Adetiba, T.C. 2017. Regional and economic security: A driver for South African National Security? *Journal of African Union Studies (JoAUS*), 6(2): 199-223.

Africa, S. 2009. The South African intelligence services: A historical perspective', In: *Changing intelligence dynamics in Africa.* eds. S. Africa & J. Kwadjo, (GFN-SSR)/ (ASSN). England: Birmingham.

African Union Convention. 2014. *Convention on cyber-security and personal data protection* Retrieved from: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (Accessed 6 June 2020)

Ali, M. 2021. Occupational health and safety Act, 1993 (Act 85 of 1993) and Occupational health and safety bill (2020). Retrieved from: https://www.linkedin.com/pulse/occupational-health-safety-act-1993-85-bill-2020-muhammad-ali/ (Accessed: 12 May 2021).

Allen, G. 2016. *Introduction to the department of homeland security. Risk analysis and management for critical asset protection*. Butterworth Heinemann: Elsevier Inc.

Alshboul, A. 2010. *Information systems security measures and countermeasures: Protecting organisational assets from malicious attacks*. Chicago: Argosy University.

Alshoubaki, W & Harris, M. 2022. *Striving for protection: Whistleblowers in Jordan*. New York: SAGE Open. https://doi.org/10.1177/21582440221095023

Alvi, M.H. 2016. *A manual for selecting sampling techniques in research. Munich personal ePEcArchive: Paper No1, 70218*. UTC Retrieved from: https://mpra.ub.uni-muenchen.de/70218/1/MPRA (Accessed on 15 June 2021}

Ameer-Mia, F. & Shacksnovis, L. 2019. Cybercrimes Bill – A positive step towards the regulation of cybercrimes in South Africa *Technology and Sourcing* 13(4): 137. Retrieved from: https://www.cliffedekkerhofmeyr.com/en/news/publications/2019/ (Accessed on 13 February 2021)

Amundrud, O., Aven, T. & Flage-First, R. 2017. How the definition of security risk can be made compatible with safety definitions. *Sage Journals*. https://doi.org/10.1177/1748006X17699145

Andales, J. 2022. *Risk assessment: Identify, analyze, and mitigate potential hazards and the risks associated with it. Safety Culture*. Retrieved from: https://safetyculture.com/topics/risk-assessment/ (Accessed on: 02 April)

Anderson, C. 2010. Presenting and evaluating qualitative research. *American Journal of Pharmaceutical Education*, 74(8): 141. https://doi.org/10.5688/aj7408141

Anderson, V. 2014. *Research methods in human resource management: Investigating a business issue*. 3rd ed. London: CIPD House.

Anderson, J. & Poole, M. 2014. *Assignment & thesis writing. South African edition*. Cape Town: Juta.

Antinyan, V, Staron, M, Sandberg, A. & Hansson, J. 2016. "A complexity measure for textual requirements", *2016 Joint Conference of the International Workshop on Software Measurement and the International Conference on Software Process and Product Measurement (IWSM-MENSURA)*.

Ary, D., Cheser-Jacobs, L., Sorensen Irvine, C.K. & Walker, D.A. 2019. *Introduction to research in education*, 10th ed. Boston: Cangage.

Asiaman, N., Mensah, H.K. & Oteng-Abayie, E.F. 2017. General, target and accessible population: Demystifying the concepts for effective sampling. *The Qualitative Report*, 22(6): 1607-1621.

Association of Certified Fraud Examiners. 2014. *Financial illicit transaction, law, prevention and deterrence and investigation*. The Gregor Building. 176 West Avenue, United States of America: Elsevier. Retrieved from: https://www.acfe.com/-/media/files/acfe/pdfs/2014-report-to-nations.ashx (Accessed on 15 June 2021).

Aurini, J.D., Heath, M. & Howells, S. 2016. The 'how to' of qualitative research. London: Sage.

Aven, T. 2010. On the need for restricting the probabilistic analysis in risk assessments to variability, *Risk Analysis*. 30(3): 354-360.

Aven, T. 2015. *Risk assessment and risk management: Review of recent advances on their foundation.* Ullanhaug: University of Stavanger.

Azad, T.B. 2008. *Securing citrix presentation server in the enterprise*. New York: Elsevier Science.

Azhar, C. 2010. Counter-terrorism and international cooperation against terrorism — An elusive goal: A South African Perspective. *South African Journal on Human Rights*, 26(35): 10-535, https://doi.org/10.1080/19962126.2010.11864998

Babbie, E. 2017. *The basics of social research*. 7th ed. USA: Cengage Learning.

Badenhorst, C. 2014. *Research writing. Breaking the barriers*. Pretoria: Van Schaik.

Bak, N. 2013. *Completing your thesis: A practical guide*. Pretoria: Van Schaik.

Basdeo, V. 2017. Criminal and procedural legal challenges of identity theft in the cyber and information age. *SAJCJ* 30: 363

Bayne, J. 2020. *An overview of threat and risk assessment*. Maryland: SANS

Beresford, A. 2015. Power, patronage, and gatekeeper politics in South Africa. *African Affairs,* 114(455): 226-248.

Berg, J. & Gabi, V. 2011. *Regulating private security in South Africa context, challenges and recommendations*. Pretoria: African Policing Civilian Oversight Forum.

Bertram, C. & Christiansen, I. 2014. *Understanding research: An introduction to reading research.* Pretoria: Van Schaik.

Bickley, S. 2017. *Security risk management: A basic guide for smaller NGOs*. England: European Interagency Security Forum (EISF).

Bishop, M. 2003. What is computer security? *IEEE Security & Privacy Magazine IEEE Secure*, 99(1): 67-69.

Black, I.S. 2010. *Defensive tactics and officer safety: The professional protection officer*. New York: Elsevier

Blackwell, A.F., Church, L. & Green, T. 2008. The abstract is 'an enemy'. In *Proc. psychology of programming interest group* (PPIG). Oxford: Butterworth-Heinemann.

Blanchard, D.C., Griebel, B. & Blanchardc, R.J. 2010. *Risk assessment as an evolved threat detection and analysis process*. Monoa: Elsevier Ltd.

Bless, C., Higson-Smith, C. & Sithole, S.L. 2014. *Fundamentals of social research methods: An African perspective.* 5th edition. Cape Town: Juta.

Bordens, K.S. & Abbott, B.B. 2014. *Research design and methods: A process approach*. 9th ed. New York: Mc Graw Hill.

Botha, M.M. & Van Heerden, C.M. 2014. The Protected Disclosures Act 26 of 2000, the Companies Act 71 of 2008 and the Competition Act 89 of 1998 with regard to blowing protection: Is there a link? *Tydskrifvir die Suid-Afrikaanse Reg*, 2014(2): 337-358.

Botha, R. & Visser, J. 2012. Forceful arrests: An overview of Section 49 of the Criminal Procedure Act 51 of 1977 and its recent amendments. *Potchefstroom Electronic Law Journal (PELJ)*, *15*(2): 01-36

Broder, J.F. & Tucker, E. 2012. *Risk analysis and the security survey. 4th ed.* Oxford: Butterworth-Heinemann

Brotby, W.K. 2008. *Information security governance: Guidance for information security managers.* Rolling Meadows: T Governance Institute.

Bryman, A. 2012. *Social research methods*. Oxford: Oxford University Press.

Burchell, J. 2006. Deadly force and fugitive justice in the balance: The old and the new face of Section 49 of the Criminal Procedure Act. *South African Journal of Criminal Justice,* 13(2): 200 – 213.

Burgess, C. 2018. *Do cybercriminals ever get extradited?* Retrieved from: https://securityboulevard.com/2018/04/do-cybercriminals-ever-get-extradited (Accessed 14 September 2020)

Business Insider SA. 2020. *Hackers on the dark web love South Africa - here's why we suffer 577 attacks per hour* Retrieved from:

https://www.businessinsider.co.za/sa-third-highest-number-of-cybercrime-victims-2020-6 (Accessed on 05 June 2020

Campbell-Young, S. 2016. *Ineffective security the result of ineffective allocation of resources*. Midrand: Phoenix Distribution.

Cawthra, G. 2019. The death of security sector reform, the South African exemplar revisited. *Conflict, Security & Development*, 19(2): 223-235 https://doi.org/10.1080/14678802.2019.1570723

Cepik, M. & Ambros, C. 2014. Intelligence, crisis, and democracy: Institutional punctuations in Brazil, Colombia, South Africa and India. *Intelligence and National Security,* 29(4): 523-551.

Chou, T.S. 2013. Security threats on cloud computing vulnerabilities. *International Journal of Computer Science & Information Technology, 5*(3): 79.

Cilliers, J. 2021. South Africa's security sector in crisis-Reform must start now. *New 24.* Retrieved from: https://www.news24.com/news24/analysis/analysis-jakkie-cilliers-south-africas-security-sector-is-in-crisis-reform-must-start-now-20210721 (Accessed: 19 February 2022).

Clough, J. 2014. *A world of difference: The Budapest Convention on cybercrime and the challenges of harmonisation*. Australia: Monash University

Cockerham, W.C. 2016. *International encyclopaedia of public health. 2nd ed*. United States of America: Elsevier.

Community Emergency Response Team (CERT). 2014. *High operating standards and professionalism*. Retrieved from: https://www.certsa.org/ (Accessed on 20 February 2021)

Corbin, J. & Strauss, A. 2015. *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Los Angeles: SAGE.

Council of Europe. 2001. *Explanatory report to the convention on cybercrime*. European Treaty Series No 185. Retrieved from: https://rm.coe.int/16800cce5b. (Accessed on 04 May 2021).

Creswell, J.W. 2014. *Research design: International student edition. 4th ed*. Washington, DC: Sage.

Crossman, A. 2019. *What is participant observation research? Understanding an important qualitative research method*. California: Science Tech Math.

Crouch, M. & McKenzie, H. 2006. The logic of small samples. In: Interview-based qualitative research. *Social Science Information*, 45 (4): 18.

Dalziel, H. 2015. *Infosec management fundamental. 1st ed*. Rockland: Syngress Publishing

Daniel, J. 2012. *Sampling essentials: Practical guidelines for making sampling choices*. Los Angeles: SAGE.

David, L. & Brydon-Miller, M. 2014. *The safe encyclopaedia of action research*. Thousand Oaks, CA: Sage Publishing.

De Vaus, D. 2013. *Research design in social research.* Los Angeles: SAGE.

Defence Science and Technology Organisation. 2010. *Technical risk assessment handbook*. Version 1.1. Canberra: Fairbairn Business Park Department of Defence.

Denscombe, M. 2014. *Research proposals: A practical guide*. Berkshire: Open University Press.

Department of International Relations and Cooperation. 2015. *Revised strategic plan*: *2015-2020.* Pretoria: DIRCO.

Department of Public Service and Administration/ DPSA. 2016. *Public Service Regulations 2016 – Part 1*: Pretoria: DPSA.

Department of Water Affairs and Forestry. 2021. Implications of Recent Legislation (*Other Than National Water Act*) on Information Requirements. Retrieved from: https://www.dws.gov.za/iwqs/wrmais/mais1/appendix5.htm (Accessed 20 February 2022)

Dhillon, G. 2006. *Principles of information systems security: Texts and cases*. 1St ed. Hoboken, New Jersey: Wiley Publishing.

Diphoko, W. 2021. *South African government entities hit by cyber attacks and services affected*. Pretoria: ILO. Retrieved from: https://www.iol.co.za/technology/sa-government-entities-hit-by-cyber-attacks-and-services-affected-6527c606-4667-4e0c-a162-16f8bc5b2f5a (Accessed: 20 February 2022).

Dlomo, T.D. 2004. 'An analysis of parliamentary intelligence oversight in South Africa with specific reference to the joint standing committee on intelligence'. Published Master's Dissertation. Pretoria: University of Pretoria.

Douglas, T. 2018. *Phishing, malware, ransomware among top public-sector threats, reports find.* Retrieved from: http://www.govtech.com/pcio/articles/Phishing-Malware-Ransomware-Among-Top-Public-Sector-Threats-Reports-Find.html. (Accessed: 20 February 2022)

Du Toit, D.F.P., Knipe, A., Van Niekerk, D., Van der Waldt, G. & Doyle, M. 2002. *Service excellence in governance.* Sandown: Heinemann.

Dudovskiy, J. 2018. *The ultimate guide to writing a dissertation in business studies: A step-by-step assistance*. Retrieved from: http://research-methodology.net/about-us/ebook/ (Accessed on 01 June 2021).

Duff, A. 2010. Can an employer dismiss due to facebook? *Packaging Review South Africa,* 36(2): 1-15

Dunn, D.S. 2013. *The practical researcher. 3rd ed*. New York: Wiley.

Durrheim, K. & Painter, D. 2016. *Research in practice: Applied methods for the social sciences. 2nd ed*. Cape Town: Juta.

Dyer, L. & Bowmans, C.K. 2021. *Digital business in South Africa: Overview. Thompson Reuters practical law*. Retrieved from: https://uk.practicallaw.thomsonreuters.com/w-007-8319?TransitionType=Default& contextData=(sc.Default)&firstPage=true. (Accessed on 13 March 2020).

Efron, S.E. & Ravid, R. 2019. *Writing literature review: A practical guide.* New York: Guilford Publication Incl.

Elo, S., Kaariainen, M., Kanste, O., Polkki, T., Utriainen, K. & Kyngas, H. 2014. Qualitative content analysis: A focus on trustworthiness. *Journal of Advanced Nursing, Science-Sage*. https://doi.org/10.1177/2158244014522633

Fay, J.J. & Patterson, D. 2018. *Contemporary security management. 4th ed*. Butterworth: Elsevier Inc.

Flick, U. 2020. *An introduction to qualitative research. 5th ed*. London: Sage.

Fruhlinger, J. 2019. *What is phishing? How this cyber attack works and how to prevent it.* Available from: https://www.csoonline.com/article/2117843/what-is-phishing? (Accessed: 20 February 2022).

Garaba, F. 2012. Public domain management of liberation movement heritage records in Eastern and Southern Africa. *African Journal Library, Archive, and Information Science, 22*(2): 33-142.

Garcia, M.L. 2006. *Vulnerability assessment of physical protection systems*. Oxford: Butterworth-Heinemann.

Garg, R. 2020. *Geeks for geeks: What is information security*. Noida: Uttar Pradesh.

Gercke, M. 2014. *Understanding cybercrime: Phenomena, challenges and legal response.* Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/legislation.aspx. (Accessed on 01 June 2021)

Govender, D. 2018. *Management security information: Incidents, threats & vulnerabilities.* Pretoria: UNISA Press.

Govender, D., Sewpersad, S. & Mahambane, M.A. 2015. *Security science programme: corporate investigation II*. Pretoria: University of South Africa.

Government of Canada. 2016. Our *Security, our rights: National security green paper*. Ottawa: Government of Canada.

Grama, J. 2011. *Legal issues in information security*. Sudbury, MA: Jones & Bartlett Learning.

Gravetter, F.J. & Forzano, L.B. 2010. *Research methods for the behavioral sciences. 6th ed*. Belmont, CA: Wadsworth.

Greenleaf, G. 2013. Sheherezade and the 101 Data privacy laws: Origins, significance and global trajectories. *Journal of Law, Information & Science*, 40. Retrieved from: http://ssrn.com/abstract=2280877. (Accessed on 20 August 2021)

Gritzalis, D., Iseppi, G., Mylonas, A. & Stavrou, V. 2018. Exiting the risk assessment maze: A meta-survey. *ACM Comput. Surv, 51*, 1–30.

Gruyter, D.E. 2021. *Project risk management: Risk-based security engineering*. Berlin: Deutsche National bibliothek.

Guest, G., Namey, E.E. & Mitchell, M.L. 2013. *Collecting qualitative data*. Los Angeles: SAGE.

Gumedze, S. 2008. Regulating the private security industry in South Africa. *Social Justice*, 34(3): 109-110.

Gutwirth, S., Leene, R., De Hert, P. & Poulett, Y. 2012. *European data protection: In good health.* London, New York: Springer Verlang Publishers.

Hammond, M. & Wellington, J.J. 2013. *Research methods: The key concepts.* New York: Routledge.

Hansson, S.O. Aven T. 2014*. Is risk analysis scientific? A model for linking the various stages in the risk informed decision-making*. New York: John Wiley & Sons, Inc.

Harbach, M., Hettig, M., Weber. & Smith, M. 2014*. Using personal examples to improve risk communication for security and privacy decisions*. Hannover: Leibniz University Hannover.

Haven, T.L. & Van Grootel, L. 2019. Preregistering qualitative research*.* Accountability in research. *Policies and quality assurance, 32*(26): 229–244.

Hayes, J. & Drury, M. 2019. *Cybersecurity in United Kingdom Lexology*. Oxford: University of Oxford

Henning, E., Gravett, S. & Van Rensburg, W. 2013. *Finding your way in academic writing*. 2nd ed. Pretoria: Van Schaik.

Henning, J.J. 2014. Some manifestations of the statutory recognition of a partnership as an entity. *Journal for Juridical Science 39*(2): 53-66.

Hennink, M., Hutter, I. & Bailey, A. 2020. *Qualitative research methods*, 2nd ed. London: Sage.

Hlengwa, M. 2019. *State security agency on vetting of officials. Research unit on audit outcomes, with minister*. Cape Town: Parliamentary Monitoring Group.

Hlongwane, S. 2013. *Securitisation of South Africa. Why should we be afraid? Daily Maverick.* Retrieved from: https://www.dailymaverick.co.za/article/2013-02-18-the-security-state-of-south-africa-why-you-should-be-afraid-very-afraid/. (Accessed on 15 May 2020)

Hull, J.C. 2018. *Risk management and financial institutions*. 5th ed. New Jersey: John Wiley & Sons, Inc., Hoboken.

Hutton, S. 2017. *Why phishing attacks are increasingly targeting the public sector (and what you can do about it).* Retrieved from: https://gcn.com/articles/2017/10/20/email-security-phishing.aspx (Accessed: 20 February 2022).

Imperva. 2021. *Vulnerability assessment. California: Application security*. Retrieved from: https://www.imperva.com/learn/application-security/vulnerability-assessment. (Accessed on 23 June 2022)

Isa, M. 2020. *SA suffers as cybercrime rises globally. Fin24*. Retrieved from: https://www.news24.com/fin24/Finweek/Business-and-economy/sa-suffers-as-cybercrime-rises-globally-20200106 (Accessed: 31 March 2022).

Isnaini, K.N. & Solikhatin, S.A. 2020. Information security analysis on physical security in university x using maturity model. *Journal Informatika*, 14(2): 76-84.

Jagatic, T.N., Johnson, N.A., Jakobsson, M. & Menczer, F. 2007. Social phishing. *Communications of the ACM*, 50(10): 94-100.

Johansen, I.L. & Rausand, M. 2014. Foundations and choice of risk metrics. *Safety Science*, 62: 386–399.

John, M. & White, J.M. 2014. *Security risk assessment: Managing physical and operational security*. London: Elsevier.

Kabanda, S.K., Brown, I., Nyamakura, V. & Keshav, J. 2010. South African banks and their online privacy policy statements: A content analysis', *SA Journal of Information Management* 12(1): 1-7 https://doi.org/10.4102/sajim.v12i1.418

Katsikas, S.K. 2013. *Computer and information security handbook: Risk management. 3rd ed*. London: Elsevier.

Kavis, M.J. 2014. *Architecting the cloud: Design decisions for cloud computing service models (SaaS, PaaS, and IaaS)*. New Jersey: John Wiley & Sons.

Khumalo, N.B., Bhebhe, S. & Mosweu, O. 2016. A comparative study of freedom of information legislation in Botswana, South Africa and Zimbabwe. *Mousaion, 34*(4): 108-131.

Knoesen, A.L. 2012. 'The use of physical surveillance in forensic investigation'. Published Master's Dissertation. Pretoria: University of South Africa.

Kumar, R. 2019. *Research methodology: A step-by-step guide for beginners*. 5th edition. Los Angeles: SAGE.

Kuzminykh, I & Carlsson, A. 2018. Analysis of assets for threat risk model in avatar-oriented iot architecture. In *internet of things, smart spaces, and next generation networks and systems*; Galinina, O., Andreev, S., Balandin, S., Koucheryavy, Y., Eds.; Springer: Cham, Switzerland, (11)118: 52–63.

Kuzminykh, I., Ghita, B., Sokolov, V. & Bakhshi, T. 2021. Information security risk assessment. *Encyclopedia,* 1: 602–617.

Lanier, M.M. & Briggs, L.T. 2014. *Research method in criminal justice and criminology. A mixed methods approach*. New York: Madison Avenue.

Lee, M.C. 2014. Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method. *Int. J. Comp. Sci. Inf. Tech. 6*: 29–45.

Leedy, P.D. & Ormrod, J.E. 2014. *Practical research planning and design:* Pearson New International edition. 10th ed. USA: Pearson.

Lemke, F. & Petersen, H.L. 2013. *Teaching reputational risk management in the supply chain*. Bingley: Emerald Group Publishing Limited.

Lohrmann, D. 2021. Data breach numbers, costs and impacts all rise in 2021. Government Technology. Retrieved from: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/data-breach-numbers-costs-and-impacts-all-rise-in-2021 (Accessed on 02 April 2020)

Luo, X. 2017. Awareness education as the key to ransomware prevention. *Information Systems Security,* 16: 195-202.

Mabasa, H.M. & Olutola, A.A. 2021. The structure of South African police: Towards a single police service. *Cogent Social Sciences, 7*(1): 2-13.

Mahlatsi, L.W. 2019. 'An exploration of the chasm in the protection of classified information in South African government departments'. Published Master's Dissertation. Pretoria: UNISA.

Maillart, J.B. 2014. The limits of subjective territorial jurisdiction in the context of cybercrime. *ERA Forum* 375.

Majid, U. 2018. *Research fundamentals: Study design, population, and sample size*. URNCST Journal. 32(1):1-7.

Mandell, A. 2013. *Security risk assessment info*. Pretoria: Alwinco.

Maree, K. 2007. *First steps in research*. Durban: Van Schaik.

Marshall, C. & Rossman, G.B. 2016. *Designing qualitative research. 6th ed*. London: Sage.

Masse, T., O'Neil, S. & Rollins, J. 2007. *The department of homeland security's risk assessment methodology: Evolution, issues, and options for congress*. Austin: Congressional Research Service.

Matzopoulos, R., Simonetti, J., Prinsloo, M., Neethling, I., Groenewald, P., Dempers, J., Martin, L.J., Rowhani-Rahbar, A., Myers, J.E. & Thompson, M.L. 2018. A retrospective time trend study of firearm and non-firearm homicide in Cape Town from 1994 to 2013. Cape Town*: South African Medical Journal*, *108*(3): 197-204

Maude, S.M. 2007. *Public Finance Management Act, 1 of 1999 – A compliance strategy.* Pretoria: University of South Africa.

Maxwell, J.A. 2013. *Qualitative research design: An interactive approach*. 3rd ed. California: SAGE Publications.

May, T. 2011. *Social research: Issues, methods and process. 4th ed*. England: Open University Press.

Mbanaso, M. 2021. *Cyber risk management*. Swindon: Link Centre.

Mbowe, J.E., Zlotnikova, I., Msanjila, S.S. & Oreku, G.S. 2014. A conceptual framework for threat assessment based on organisation's information security policy. *Journal of Information Security, 5*: 166-177.

Mbuvi, D. 2011. *African states urged to ratify Budapest cybercrime convention*. London: SAGE Publications.

McDowell, W.H. 2013. *Historical research: A guide*. New York: Routledge.

Mdluli, B.D. 2011. *Fundamentals of security vetting in a democratic South Africa*. Cape Town: JM Productions.

Merriam, S. B. & Tisdell, E.J. 2016. *Qualitative research: A guide to design and implementation,* 4th ed*.* San Francisco: Wiley.

Mills, R.F., Grimaila, M.R., Peterson, G.J. & Butts, J.W. 2011. *A scenario-based approach to mitigating the insider threat*. Dayton: ISSA.

Moagi, N.J. 2009. *Evaluating compliance of Public Finance Management Act by the Department of Labour in Limpopo Province*. Polokwane: University of Limpopo.

Mohlabeng, T. 2020. Undocumented immigrants pose a threat to SA's national security. *ILO*. Retrieved from: https://www.iol.co.za/the-star/opinion-analysis/opinion-undocumented-immigrants-pose-threat-to-sas-national-security-da0de0eb-5fc0-463c-9ecb-254aa0ce5401 (Accessed: 18 February 2022).

Monzon, L. 2021. SA data breach costs reached record highs during pandemic – IBM. IT News Africa. Retrieved from: https://www.itnewsafrica.com/2021/08/sa-data-breach-costs-reached-record-highs-during-pandemic-ibm/ (Accessed on 02 April 2022)

Mouton, J. 2014. *Understanding social research*. Pretoria: Van Schaik.

Murphy, D. & Randall, W.F. 2016. *Workplace safety: Establishing an effective violence prevention program*. Butterworth: Elsevier Inc.

NASP School Safety and Crisis Response Committee. 2014. *Threat assessment for school administrators and crisis teams*. Bethesda, MD: National Association of School Psychologists.

Nathan, L. 2009a. Intelligence in South Africa: Spies threaten democracy. *The World Today, 8/9*(65): 26-28.

Nathan, L. 2009b. Lighting up the intelligence community: An agenda for intelligence reform in South Africa. *African Security Review, 18*(1): 91-104.

Nathan, L. 2012. A critique of the general intelligence law amendment. Retrieved from: http://www.politicsweb.co.za. (Accessed on: 5 May 2022).

National Crime Registrar. 2020. Crime must fall: Functionality of crime information management and analysis centre at station level. Retrieved from: https://www.saps.gov.za/resource_centre/publications/brig_manamela_assessment_functionality_of_CIMAC_at_station_level.pdf (Accessed on 17 August 2021).

National Terrorism Advisory Committee. 2014. National terrorism advisory system. Retrieved from: https://www.dhs.gov/national-terrorism-advisory-system

Nayab, N. 2020. *How to determine validity in qualitative research. Project management methods and ideologies*. USA: Bright Hub PM.

Netshakhuma, N.S. 2019. The role of archives and records management legislation after colonialism in Africa case of Southern Africa. *Records Management Journal*, https:// doi.org/10.1108/RMJ-09-2018-0024

Nkuna, J.T. 2020. 'An exploration of vetting investigation in the South African Police Service. MA Dissertation'. Pretoria: UNISA.

Nkwana, M. & Govender, D. 2017. Protection of security information in government departments: A South African case study. *Acta Criminologica: African Journal of Criminology & Victimology*, 35(5): 1-20.

Nkwana, M.J. 2015. 'Protection of security information within the government departments of South Africa'. Published Master's Dissertation. Pretoria: UNISA.

Nobanee, H., Alhajjar, M., Abushairah, G. & Al Harbi, S. 2021. *Reputational risk and sustainability: A bibliometric analysis of relevant Literature*. Basel: MDPI.

Noble, H. & Heale, R. 2019. *Triangulation in research, with examples*. Belfast: Evidence Based Nursing.

Nyanchama, M. 2005. Enterprise vulnerability management and its role in information security management. *Information Systems Security*, (14): 29-56.

Odendal, N. 2021. Cable theft and vandalism costing economy R187 billion. Engineering news. Retrieved from: https://www.engineeringnews.co.za/article/cable-theft-and-vandalism-costing-economy-r187bn-2021-07-26/rep_id:4136. (Accessed on 5 May 2022).

Onwubiko, C. & Lenaghan, A.P. 2007. *Managing security threats and vulnerabilities for small to medium enterprises*. New York: Institute of Electrical and Electronics Engineers (IEEE) Publishing.

Palmer, D. 2016. *Government is hit by 9,000 security breaches a year-but reporting them remains chaotic*. Britain: Z.D Net.

Patel, D.A. & Bharadwaj, S. 2020. *Budapest convention on cyber-crime*, 2020. Retrieved from: https://studymaterial.unipune.ac.in:8080/jspui/bitstream/12345678 (Accessed on 5 May 2022).

Patil, S.G. 2019. How to plan and write a budget for research grant proposal. *Journal of Ayurveda and Integrative Medicine.* Bangalore: Elsevier B.V.

Patrick, H., van Niekerk, B. & Fields, Z. 2016. Security-information flow in the South African Public Sector. *Journal of Information Warfare*, *15*(4): 68–85

Philpott, D. 2013. *Security consulting. 4th ed*. Oxford: Butterworth-Heinemann.

Pinnock, B. 2020. *What recent data breaches tell us about cybersecurity in South Africa* BusinessTech Retrieved from: https://businesstech.co.za/news/industry-news/433797/what-recentdata-breaches-tell-us-about-cybersecurity-in-south-africa/ (Accessed 30 September 2021).

Public Safety Canada. 2019. *Statement from ministers Goodale, Lametti and Sajjan on the passage of Bill C-59 in Parliament*. Ottawa: Government of Canada.

Raacke, J.B. & Raacke, J. 2012. *Research methods*. Boston: Pearson.

Rader, E., Wash, R. & Brooks, B. 2012. *Stories as informal lessons about security*. London: SOUPS.

Ramluckan, T. 2019. *The applicability of the Tallinn manuals to South Africa.* 14th International Conference on Cyber Warfare and Security (ICCWS) (2019) 348-355 Retrieved from: https://www.proquest.com/openview/ac4cc9f3edd6ada5ae1cfe8 (Accessed 12 May 2020)

Rees, C. 2016. *Rapid research methods for nurses, midwives and health professionals.* United Kingdom: Wiley.

Renfroe, N.A. & Smith, J.L. 2016. *Threat/ vulnerability assessments and risk analysis*. *Applied research associates*. Retrieved from: https://www.wbdg.org/resources/threat-vulnerability-assessments-and-isk-analysis. (Accessed: (14 April 2021)

Right2Know Campaign, 2017. *R2K submission on the Cybercrimes Bill*. Retrieved from: https://www.R2k.Org.Za/2017/08/11/R2k-Submission-on-the-Cybercrimes-Bill-2017 (Accessed 23 December 2020)

Rishi, V. 2019. *Cyber security breaches survey 2019. UK statistics authority, Britain.* Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/ Accessed 23 December 2020)

Ritchie, J., Lewis, J., McNaughton, C. & Ormston, N.R. 2014. *Qualitative research practice: A guide for social science students and research. 2nd ed*. London: SAGE.

Rogers, R. 2008. *Nessus network auditing.* 2nd ed. Rockland: Syngress Publishing.

Rosencrance. 2022. *Vulnerability assessment: Vulnerability analysis*. Newton: TechTarget. Retrieved from https://www.techtarget.com/searchsecurity/definition/ (Accessed on the 23 June 2022).

Ruel, E.E., Wagner, W.E & Gillespie, B.J. 2016. *The practice of survey research: Theory and applications*. London: Sage.

Sahoo, N. 2021. *Is your organisation secured from cyber risk? New York: VISTA InfoSec*. Retrieved from: https://www.vistainfosec.com/blog/types-of-vulnerability-assessment/ (Accessed on the 28 June 2022)

Saleh, Z.I., Refai, H. & Mashhour, A. 2011. *Framework for security risk assessment: faculty of computer science and information systems*. New York: Springer Publications.

SAPS. 2011. *Annual report 2010/11*. Retrieved from: https://www.saps.gov.za/about/stratframework/annual_report/2010_2011/7_prg5_protection_security_services.pdf (Accessed on the 28 June 2022)

Sharma, R. 2020. *Legislation related to cyber crimes in United Kingdom*. Retrieved from: https://www.researchgate.net/publication/347439774 (Accessed 15 January 2021)

Singh, D. 2019. Policing for safe cities and citizen security in urban South Africa. A fundamental human right. *Just Africa, 1*: 6-14.

Smith, C.L. & Brooks, D.J. 2013. *Security science: The theory and practice of security*. Butterworth: Elsevier Inc.

Smith, R. 2019. *The international comparative legal guide to cybersecurity. A practical cross-border insight into cybersecurity work*. 2nd ed. 29: 185-191. Malaysia: Global Legal Group.

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

Sotic, A., Mitrovic. V., Rajic. R. 2014. Risk perception during construction works execution. *The Online Journal of Applied Knowledge Management 2*(3), 44-55.

South Africa. 1977. Criminal Procedure Act (Act no. 51 of 1977). South Africa. 1993. Pretoria: Government Printers.

South Africa. 1980. The National Key Points Act (Act No 102 of 1980). Pretoria: South African Government.

South Africa. 1985. Control of Access to Public Premises and Vehicles Act 53 of 1985 (CAPPVA). Pretoria: South African Government.

South Africa. 1993. Occupational Health and Safety Act (Act No. 85 of 1993). Pretoria: Government Printers.

South Africa. 1994. National Strategic Intelligence Act (Act No. 39 of 1994). Government Gazette 161228. Pretoria: Government Printers.

South Africa. 1995. Labour Relations Act. Pretoria: Government Printers.

South Africa. 1996. The Constitution of the Republic of South Africa, 1996. Pretoria: Government Printer. 71

South Africa. 1998. Minimum Information Security Standards. Pretoria: Government Printer.

South Africa. 2001. Private Security Industry Regulatory Act (PSIRA) (No. 56 of 2001). Pretoria: South African Government.

South Africa. 2013. Protection of Personal Information Act. (Act No. 2013). Pretoria: Government Printer.

South Africa. 2015. BRICS (Brazil, Russia, India, China, South Africa). Retrieved from: https://www.gov.za (Accessed 19 April 2021).

South Africa. 2016. Government Gazette 40487 of 9 December 2016. 'Cybercrimes and Cybersecurity Bill' Republic of South Africa.

South Africa. 2017. Cybercrimes and Cybersecurity Bill: Republic of South Africa 2017: General Notice 871 in Government Gazette 40487 of 9 December 2016.

Southern African Migration Project. 2016. Criminal tendencies: Immigrants and illegality in South Africa. Migration Policy Brief No. 10. Retrieved from: https://samponline.org/wp-content/uploads/2016/10/brief10.pdf (Accessed: 20 February 2020).

Southern African Legal Information Institute. 2018. My Vote Counts NPC v Minister of Justice and Correctional Services and Another. 2018 (5) SA 380 (CC). Retrieved from: http://www.saflii.org/za/cases/ZACC/2018/17.html (Accessed: 20 February 2020).

Surju, J. 2018. 'A case study exploring how middle managers implement deliberate strategy in a government department'. Unpublished Master's Dissertation. Pretoria: UNISA.

Sutherland, E. 2017. Governance of cybersecurity – the case of South Africa. *The African Journal of Information and Communication (AJIC)*, 20: 83-112.

Sutton, F.S. 2015. *Process risk and reliability management: operational integrity management. 2nd ed.* London: Gulf Professional Publishing.

Tavakoli, H. 2012. *A dictionary of research methodology and statistics in applied linguistics*. Iran: Rahnama press.

Taylor, L. & Shepherd, M. 2008. *In FISMA Certification and accreditation handbook*. Amsterdam: Syngress.

Thanh, N.C. & Thanh, T.T.L. 2015. The interconnection between interpretivist paradigms and qualitative methods in education. *American Journal of Educational Science*, 1(2): 24-27.

Thoka, E.M. 2020. ‘An evaluation of security of security threats and vulnerabilities to a national key point: Case study of Medupi power station’. Unpublished Thesis Pretoria: UNISA.

Thomas, G. 2013. *How to do your research project: A guide for students in education and applied social sciences.* 2nd edition. London: Sage.

Thomashausen, A. 2007. ‘Knowing the role of international law and the United Nations’ instruments in combating and prosecuting terrorism’. Pretoria: IQPCC Conference.

Thompson, E.E. 2019. *The insider threat assessment and mitigation of risks*. New York: CRC Press.

Tight, M. 2017. *Understanding case study research: Small-scale research with meaning.* London: Sage.

Tilley, N. & Laycock, G. 2018. Developing a knowledge base for crime prevention: Lessons learned from the British experience. *Crime Prevention and Community Safety, 20*(4): 228-242.

Trochimm, W.M.K. 2020. Changes and additions. In Troy, C. 2020. *A quick guide to descriptive research*. London: Research Prospect.

Troy, C. 2020. *A quick guide to descriptive research*. London: Research Prospect.

Turianskyi, Y. 2018. Balancing cyber security and internet freedom in Africa. *Africa Portal Journal*, (31): 14-24.

UNISA. 2020. *University of South Africa COVID-19 position statement on research ethics.* Pretoria: UNISA.

Vellani, K.H. 2020. *Strategic security management a risk assessment: Guide for decision makers*. 2nd ed. New York: CRC Press.

Wagner, C., Kawulich, B. & Garner, M. 2012. *Doing social research: Global context*. United Kingdom: McGraw-Hill Education.

Walliman, N. 2015. *Research methods. the basics*. Abingdon: Routledge Publisher.

Warren, C.A.B. & Karner, T.X. 2015. *Discovering qualitative methods. Ethnography, Interviews, documents and images.* Guilford Press: New York.

Watts, S. 2017. IT *security vulnerability vs threat vs risk: What’s the difference*? Phoenix: University of Phoenix.

Welman, C., Kruger, F. & Mitchell, B. 2012. *Research methodology. 3rd ed*. Cape Town: Oxford University press.

Whitman, M.E & Mattord, H.J. 2015. *Principles of information security. 5th ed*. Georgia: Kennesaw State University.

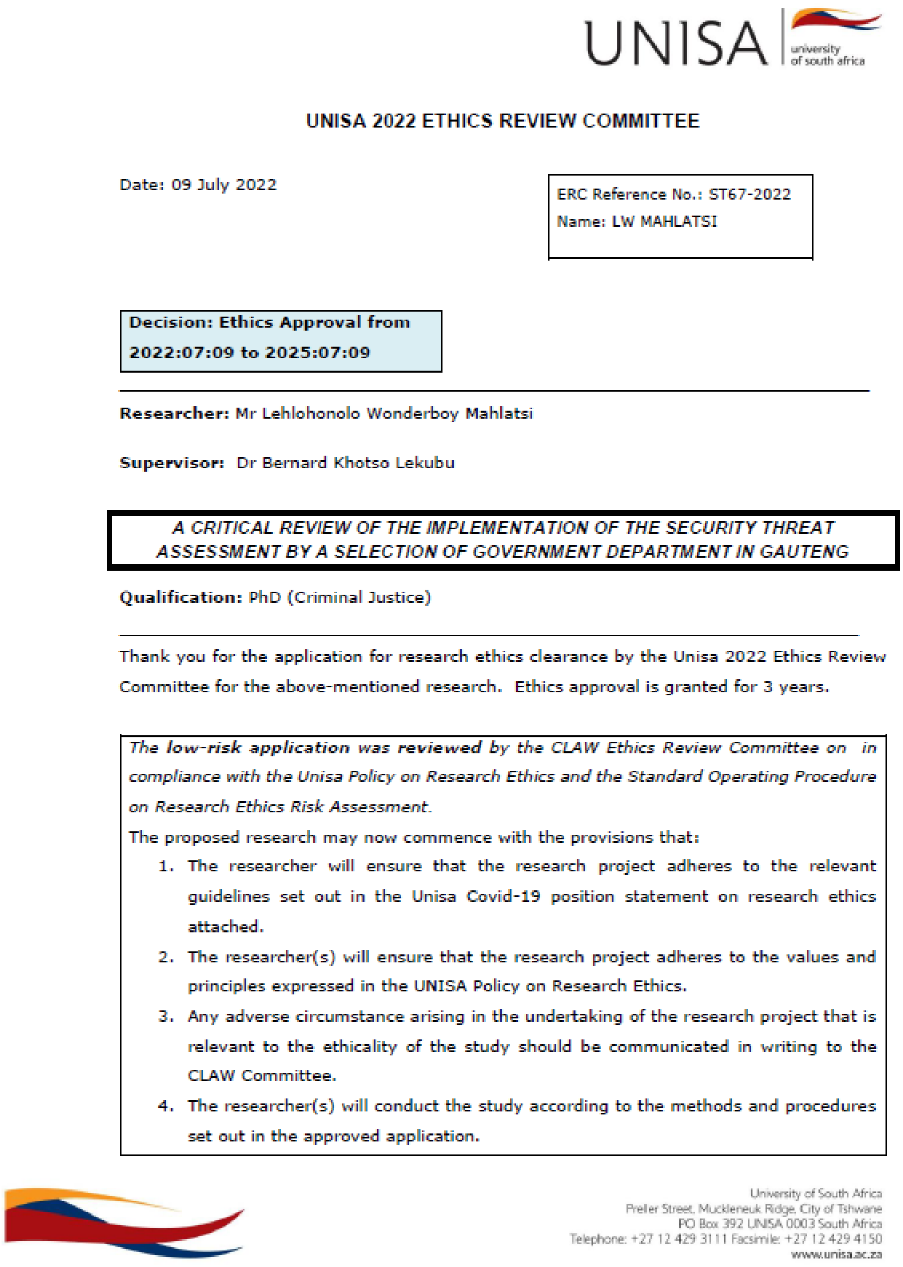
Williams, J. 2017. *Rigorous risk management a must-have for public sector organisations*. Retrieved from: Rigorous risk management a must-have for public sector organisations | ACCA Global (Accessed on 02 April 2022)

Word, S. 2019. *Assets definition: Are your assets current, fixed or intangible & what are they worth?* California: SAGE.

Yamagata-Lynch, L.C. 2010. *Activity systems analysis methods: Understanding complex learning environments*. New York: Springer Publications.

Yin, R.K. 2018. *Case study research and applications: Designs and methods*. 6th edition. LA: Sage.

ANNEXURE 1: UNISA ETHICS CLEARANCE CERTIFICATE



UNISA 2022 ETHICS REVIEW COMMITTEE

Date: 09 July 2022

ERC Reference No.: ST67-2022
Name: LW MAHLATSI

Decision: Ethics Approval from 2022:07:09 to 2025:07:09

Researcher: Mr Lehlohonolo Wonderboy Mahlatsi

Supervisor: Dr Bernard Khotso Lekubu

A CRITICAL REVIEW OF THE IMPLEMENTATION OF THE SECURITY THREAT ASSESSMENT BY A SELECTION OF GOVERNMENT DEPARTMENT IN GAUTENG

Qualification: PhD (Criminal Justice)

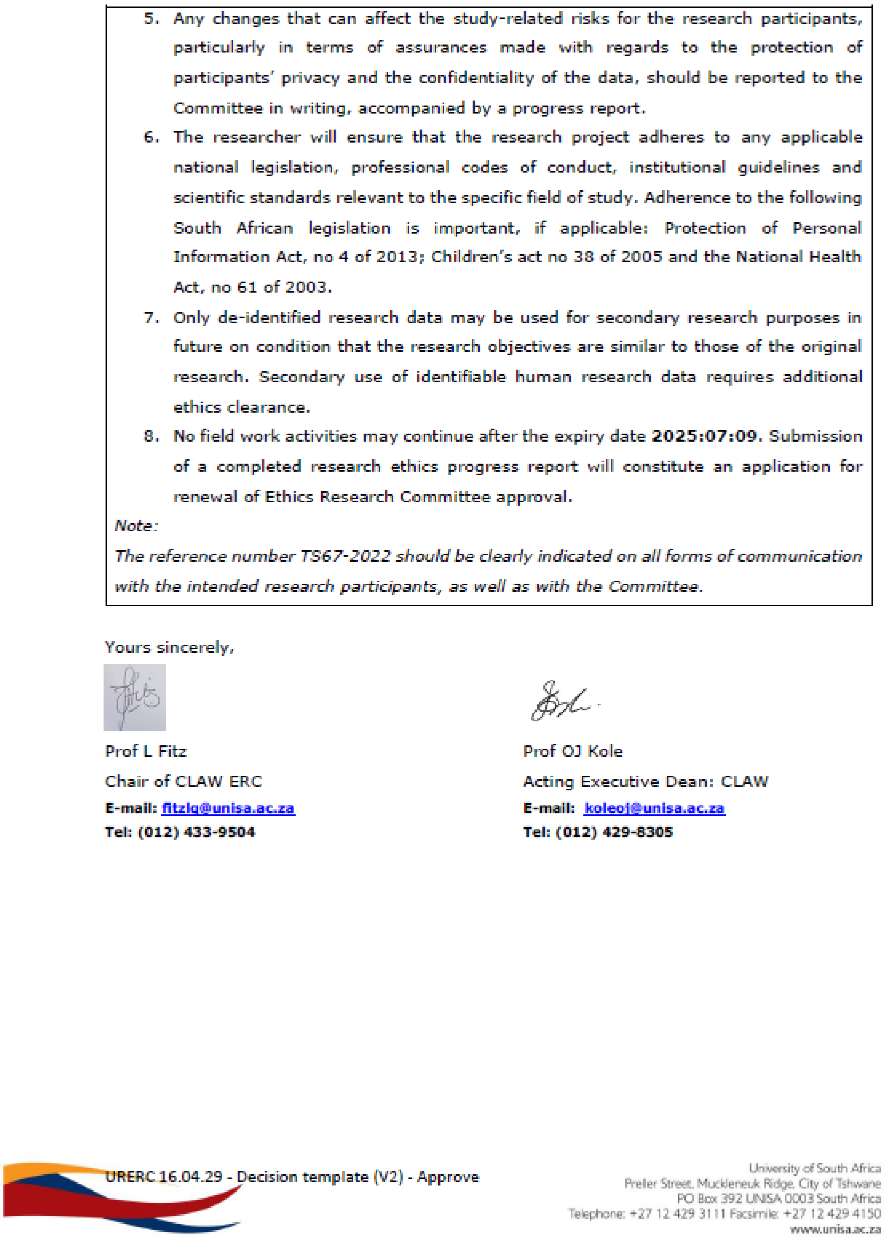
Thank you for the application for research ethics clearance by the Unisa 2022 Ethics Review Committee for the above-mentioned research. Ethics approval is granted for 3 years.

*The **low-risk application was reviewed** by the CLAW Ethics Review Committee on in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment.*

The proposed research may now commence with the provisions that:

1. The researcher will ensure that the research project adheres to the relevant guidelines set out in the Unisa Covid-19 position statement on research ethics attached.
2. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
3. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the CLAW Committee.
4. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za



5. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
6. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
7. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data requires additional ethics clearance.
8. No field work activities may continue after the expiry date **2025:07:09**. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.

Note:

The reference number TS67-2022 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.

Yours sincerely,

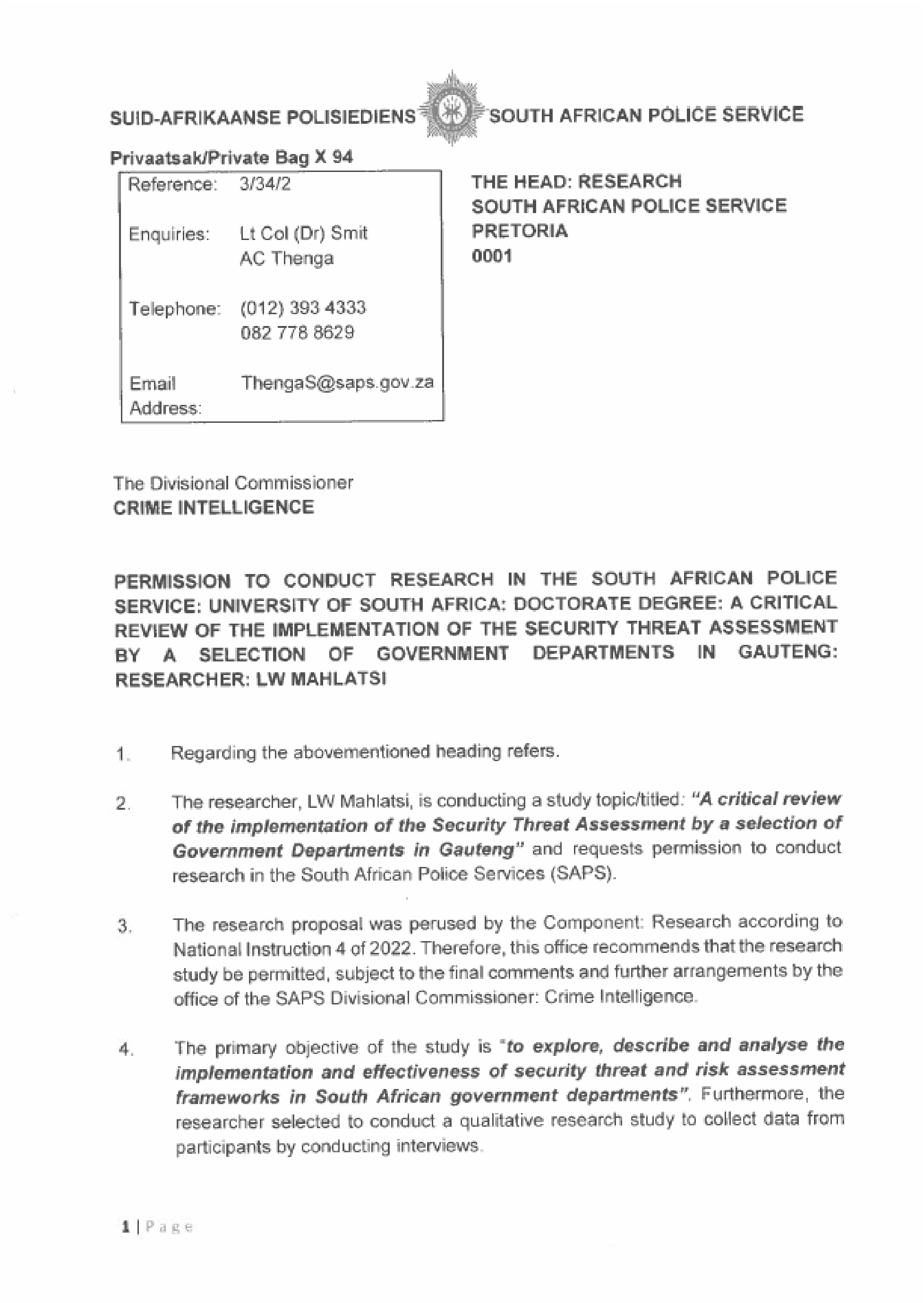
Prof L Fitz
Chair of CLAW ERC
E-mail: fitzlg@unisa.ac.za
Tel: (012) 433-9504

Prof OJ Kole
Acting Executive Dean: CLAW
E-mail: koleoj@unisa.ac.za
Tel: (012) 429-8305

URERC 16.04.29 - Decision template (V2) - Approve

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

ANNEXURE 2: SAPS APPROVAL LETTER



SUID-AFRIKAANSE POLISIEDIENS SOUTH AFRICAN POLICE SERVICE

Privaatsak/Private Bag X 94

Reference:	3/34/2
Enquiries:	Lt Col (Dr) Smit AC Thenga
Telephone:	(012) 393 4333 082 778 8629
Email Address:	ThengaS@saps.gov.za

THE HEAD: RESEARCH
SOUTH AFRICAN POLICE SERVICE
PRETORIA
0001

The Divisional Commissioner
CRIME INTELLIGENCE

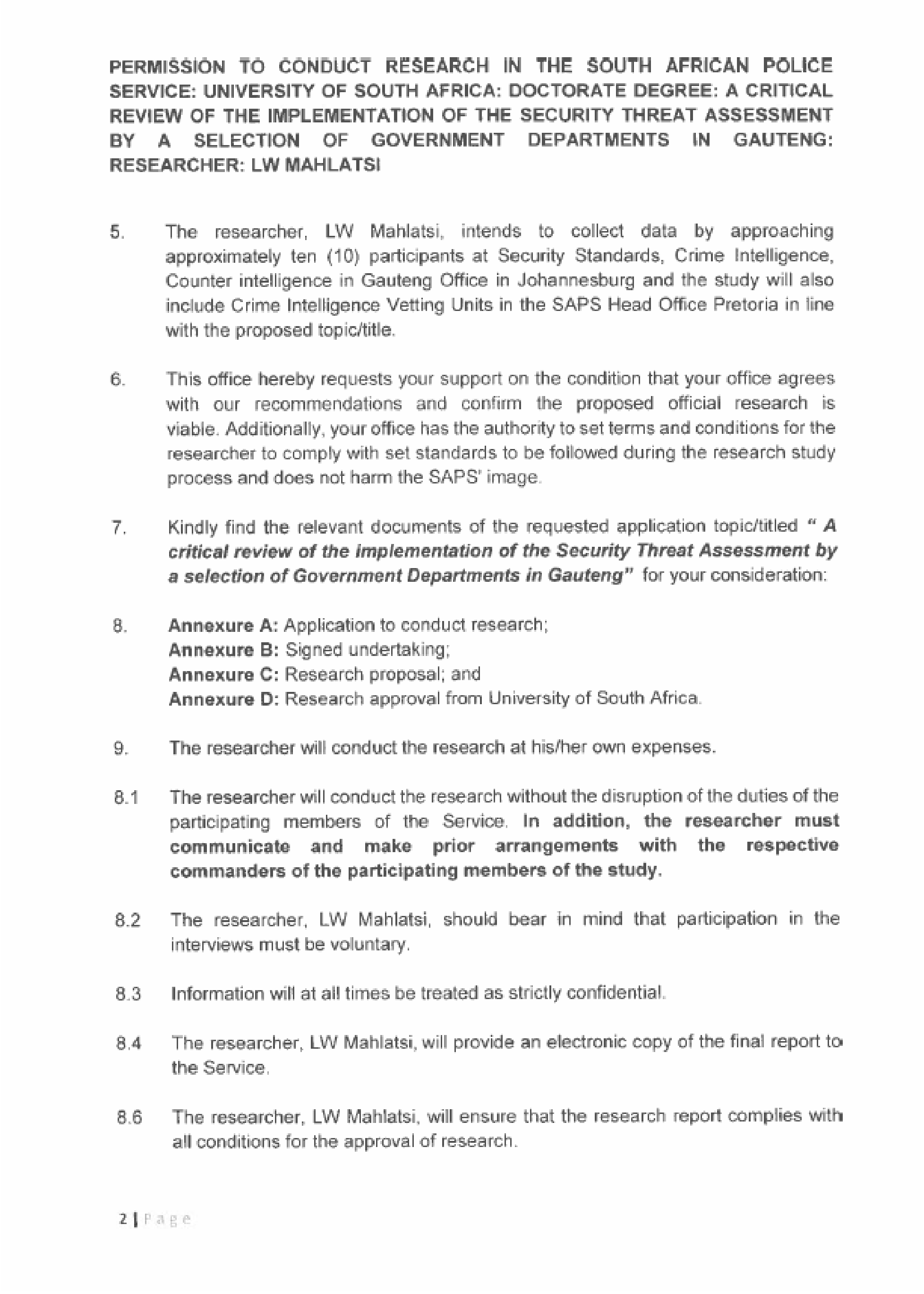
PERMISSION TO CONDUCT RESEARCH IN THE SOUTH AFRICAN POLICE SERVICE: UNIVERSITY OF SOUTH AFRICA: DOCTORATE DEGREE: A CRITICAL REVIEW OF THE IMPLEMENTATION OF THE SECURITY THREAT ASSESSMENT BY A SELECTION OF GOVERNMENT DEPARTMENTS IN GAUTENG: RESEARCHER: LW MAHLATSI

1. Regarding the abovementioned heading refers.

2. The researcher, LW Mahlatsi, is conducting a study topic/titled: ***"A critical review of the implementation of the Security Threat Assessment by a selection of Government Departments in Gauteng"*** and requests permission to conduct research in the South African Police Services (SAPS).

3. The research proposal was perused by the Component: Research according to National Instruction 4 of 2022. Therefore, this office recommends that the research study be permitted, subject to the final comments and further arrangements by the office of the SAPS Divisional Commissioner: Crime Intelligence.

4. The primary objective of the study is "***to explore, describe and analyse the implementation and effectiveness of security threat and risk assessment frameworks in South African government departments***". Furthermore, the researcher selected to conduct a qualitative research study to collect data from participants by conducting interviews.



PERMISSION TO CONDUCT RESEARCH IN THE SOUTH AFRICAN POLICE SERVICE: UNIVERSITY OF SOUTH AFRICA: DOCTORATE DEGREE: A CRITICAL REVIEW OF THE IMPLEMENTATION OF THE SECURITY THREAT ASSESSMENT BY A SELECTION OF GOVERNMENT DEPARTMENTS IN GAUTENG: RESEARCHER: LW MAHLATSI

5. The researcher, LW Mahlatsi, intends to collect data by approaching approximately ten (10) participants at Security Standards, Crime Intelligence, Counter intelligence in Gauteng Office in Johannesburg and the study will also include Crime Intelligence Vetting Units in the SAPS Head Office Pretoria in line with the proposed topic/title.

6. This office hereby requests your support on the condition that your office agrees with our recommendations and confirm the proposed official research is viable. Additionally, your office has the authority to set terms and conditions for the researcher to comply with set standards to be followed during the research study process and does not harm the SAPS' image.

7. Kindly find the relevant documents of the requested application topic/titled ***" A critical review of the implementation of the Security Threat Assessment by a selection of Government Departments in Gauteng"*** for your consideration:

8. **Annexure A:** Application to conduct research;
Annexure B: Signed undertaking;
Annexure C: Research proposal; and
Annexure D: Research approval from University of South Africa.

9. The researcher will conduct the research at his/her own expenses.

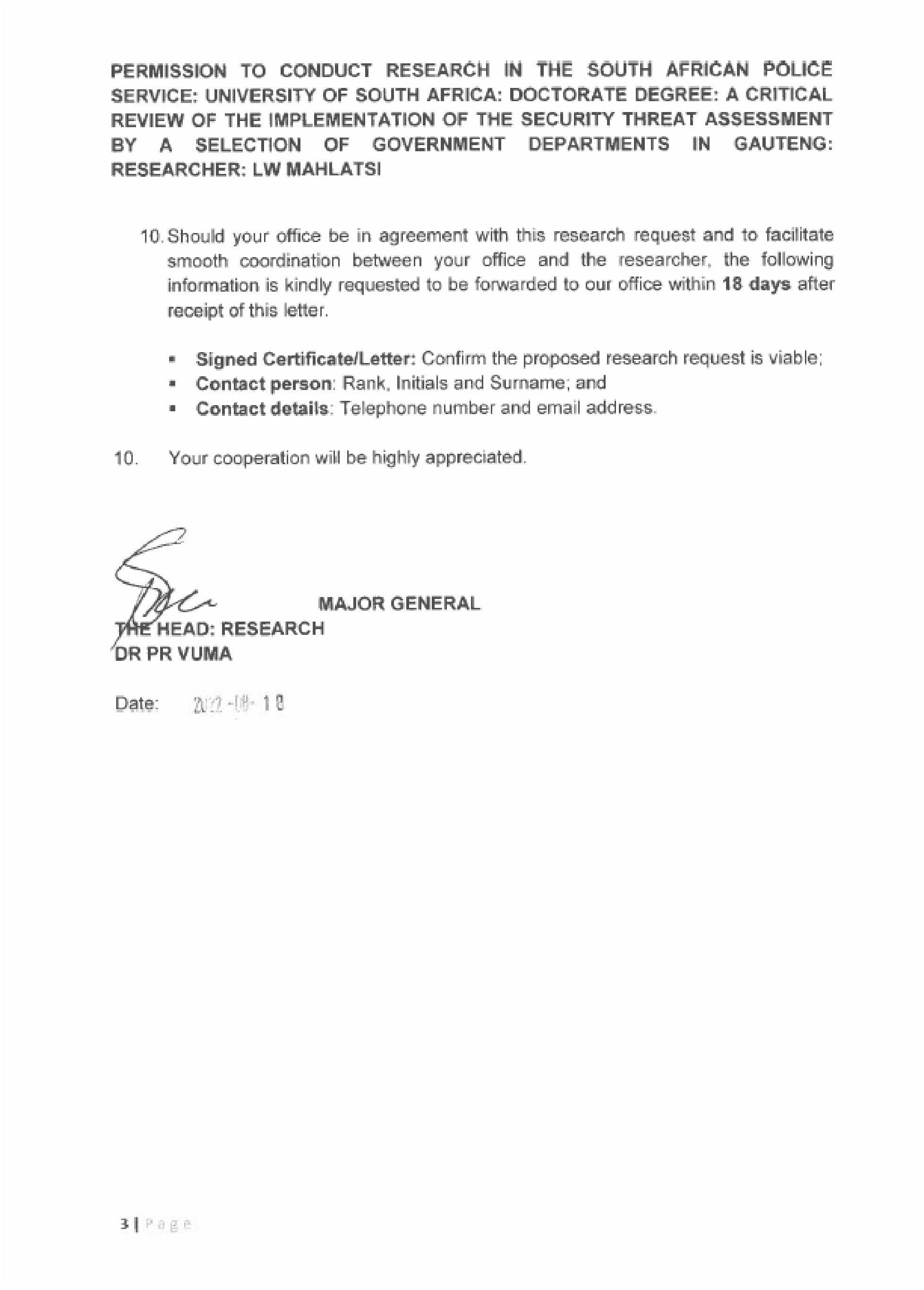
8.1 The researcher will conduct the research without the disruption of the duties of the participating members of the Service. **In addition, the researcher must communicate and make prior arrangements with the respective commanders of the participating members of the study.**

8.2 The researcher, LW Mahlatsi, should bear in mind that participation in the interviews must be voluntary.

8.3 Information will at all times be treated as strictly confidential.

8.4 The researcher, LW Mahlatsi, will provide an electronic copy of the final report to the Service.

8.6 The researcher, LW Mahlatsi, will ensure that the research report complies with all conditions for the approval of research.



PERMISSION TO CONDUCT RESEARCH IN THE SOUTH AFRICAN POLICE SERVICE: UNIVERSITY OF SOUTH AFRICA: DOCTORATE DEGREE: A CRITICAL REVIEW OF THE IMPLEMENTATION OF THE SECURITY THREAT ASSESSMENT BY A SELECTION OF GOVERNMENT DEPARTMENTS IN GAUTENG: RESEARCHER: LW MAHLATSI

10. Should your office be in agreement with this research request and to facilitate smooth coordination between your office and the researcher, the following information is kindly requested to be forwarded to our office within **18 days** after receipt of this letter.

   - **Signed Certificate/Letter:** Confirm the proposed research request is viable;
   - **Contact person**: Rank, Initials and Surname; and
   - **Contact details**: Telephone number and email address.

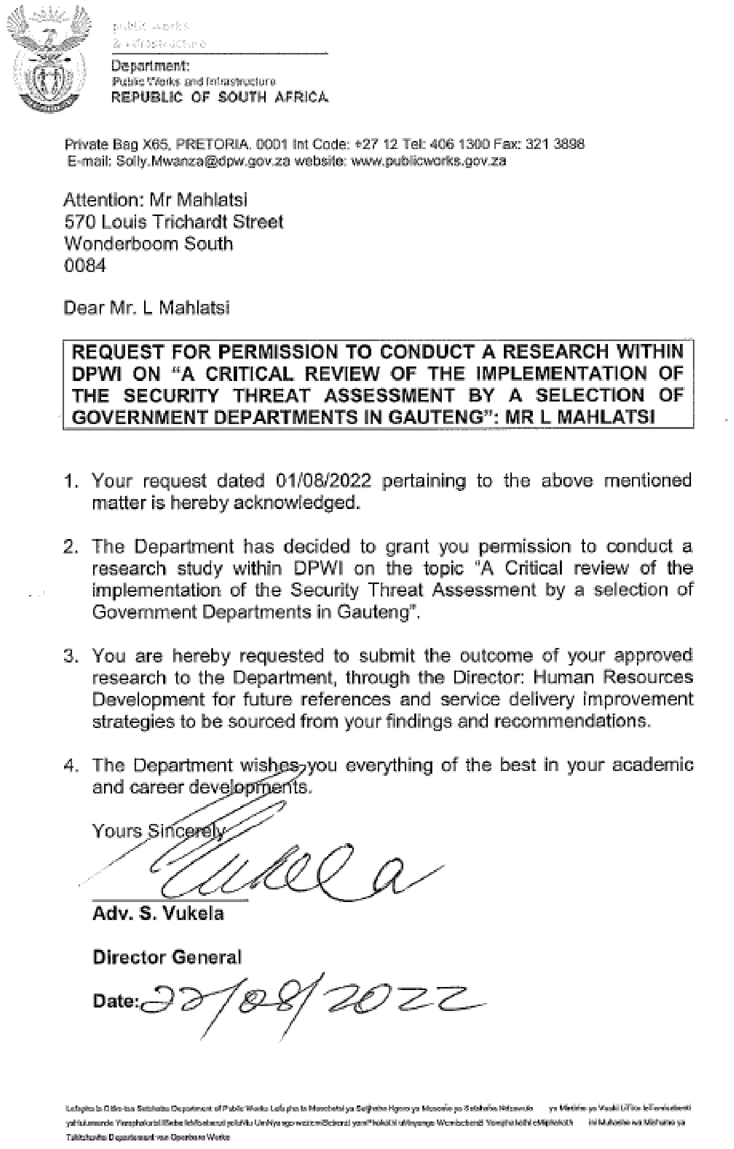
10. Your cooperation will be highly appreciated.

MAJOR GENERAL

THE HEAD: RESEARCH
DR PR VUMA

Date: 2022 -08- 18

ANNEXURE 3: LETTER TO DEPARTMENT OF PUBLIC WORKS FOR PERMISSION TO CONDUCT THE STUDY



public works
& infrastructure

Department:
Public Works and Infrastructure
REPUBLIC OF SOUTH AFRICA

Private Bag X65, PRETORIA. 0001 Int Code: +27 12 Tel: 406 1300 Fax: 321 3898
E-mail: Solly.Mwanza@dpw.gov.za website: www.publicworks.gov.za

Attention: Mr Mahlatsi
570 Louis Trichardt Street
Wonderboom South
0084

Dear Mr. L Mahlatsi

REQUEST FOR PERMISSION TO CONDUCT A RESEARCH WITHIN DPWI ON "A CRITICAL REVIEW OF THE IMPLEMENTATION OF THE SECURITY THREAT ASSESSMENT BY A SELECTION OF GOVERNMENT DEPARTMENTS IN GAUTENG": MR L MAHLATSI

1. Your request dated 01/08/2022 pertaining to the above mentioned matter is hereby acknowledged.
2. The Department has decided to grant you permission to conduct a research study within DPWI on the topic "A Critical review of the implementation of the Security Threat Assessment by a selection of Government Departments in Gauteng".
3. You are hereby requested to submit the outcome of your approved research to the Department, through the Director: Human Resources Development for future references and service delivery improvement strategies to be sourced from your findings and recommendations.
4. The Department wishes you everything of the best in your academic and career developments.

Yours Sincerely

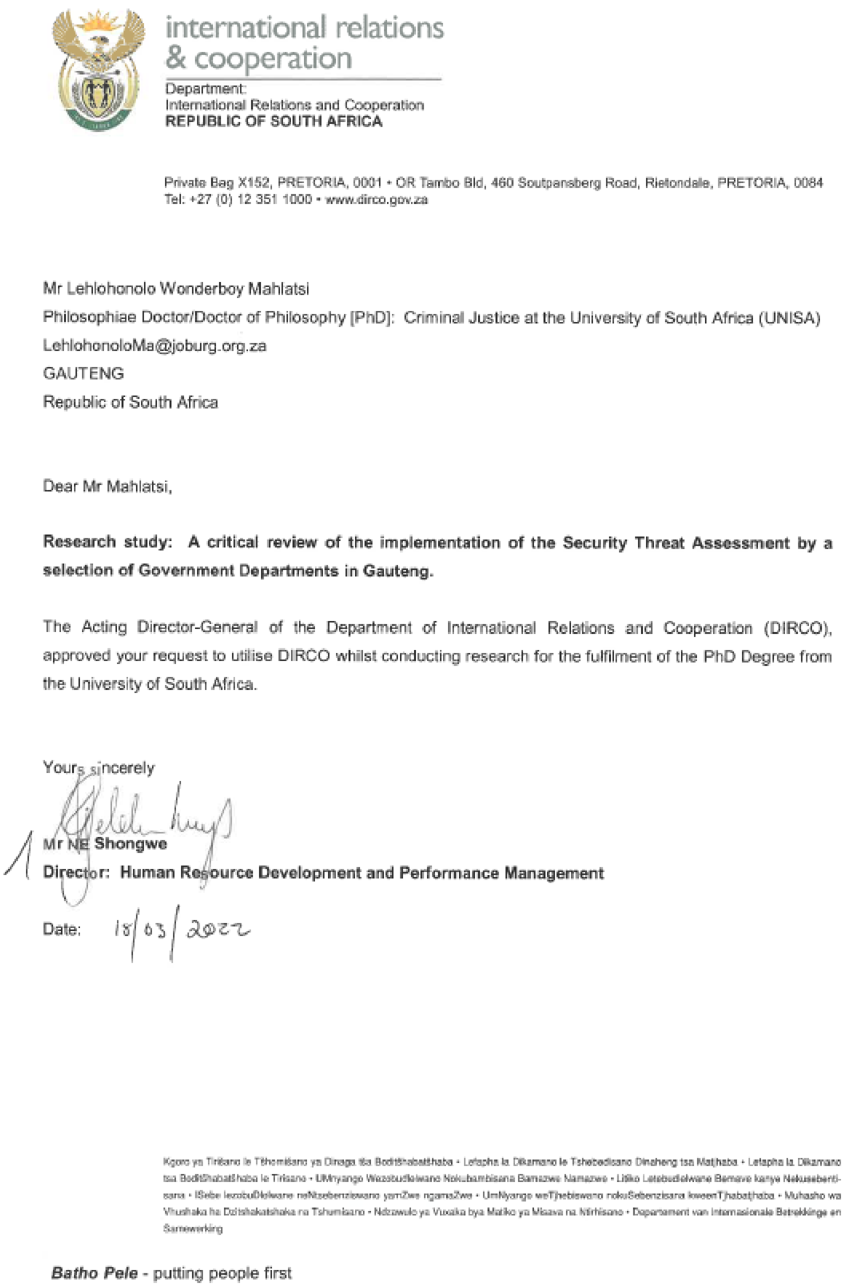
Adv. S. Vukela

Director General

Date: 22/08/2022

Lefapha la Ditiro tsa Setshaba Department of Public Works Lefapha la Mesebetsi ya Setjhaba [illegible] ya Mesebetsi ya Setshaba Ndzawulo ya Mintirho ya Vaaki [illegible] yaHulumende [illegible] [illegible] Departement van Openbare Werke

ANNEXURE 4: DIRCO APPROVAL TO CONDUCT THE STUDY



international relations
& cooperation
Department:
International Relations and Cooperation
REPUBLIC OF SOUTH AFRICA

Private Bag X152, PRETORIA, 0001 • OR Tambo Bld, 460 Soutpansberg Road, Rietondale, PRETORIA, 0084
Tel: +27 (0) 12 351 1000 • www.dirco.gov.za

Mr Lehlohonolo Wonderboy Mahlatsi
Philosophiae Doctor/Doctor of Philosophy [PhD]: Criminal Justice at the University of South Africa (UNISA)
LehlohonoloMa@joburg.org.za
GAUTENG
Republic of South Africa

Dear Mr Mahlatsi,

Research study: A critical review of the implementation of the Security Threat Assessment by a selection of Government Departments in Gauteng.

The Acting Director-General of the Department of International Relations and Cooperation (DIRCO), approved your request to utilise DIRCO whilst conducting research for the fulfilment of the PhD Degree from the University of South Africa.

Yours sincerely

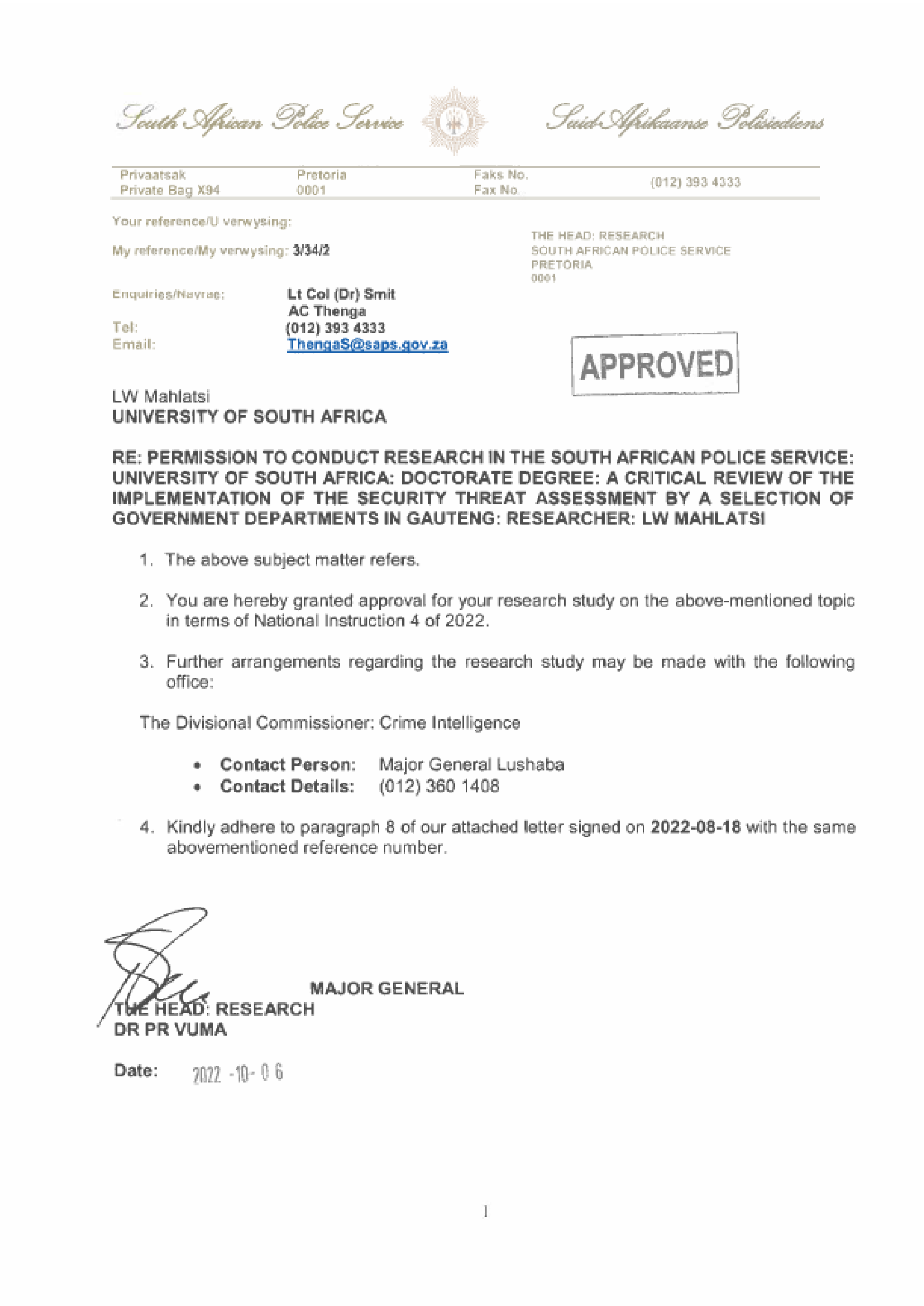
Mr NE Shongwe
Director: Human Resource Development and Performance Management

Date: 18/03/2022

Kgoro ya Tirišano le Tšhomišano ya Dinaga tša Boditšhabatšhaba • Lefapha la Dikamano le Tshebedisano Dinaheng tsa Matjhaba • Lefapha la Dikamano tsa Boditšhabatšhaba le Tirisano • UMnyango Wezobudlelwano Nokubambisana Bamazwe Namazwe • Litiko Letebudlelwane Bemave kanye Nekusebentisana • ISebe lezobuDlelwane neNtsebenziswano yamZwe ngamaZwe • UmNyango weTjhebiswano nokuSebenzisana kweenTjhabatjhaba • Muhasho wa Vhushaka ha Dzitshakatshaka na Tshumisano • Ndzawulo ya Vuxaka bya Matiko ya Misava na Ntirhisano • Departement van Internasionale Betrekkinge en Samewerking

Batho Pele - putting people first

ANNEXURE 5: SAPS APPROVAL TO CONDUCT THE STUDY



South African Police Service   Suid-Afrikaanse Polisiediens

Privaatsak Private Bag X94	Pretoria 0001	Faks No. Fax No.	(012) 393 4333

Your reference/U verwysing:

My reference/My verwysing: 3/34/2

THE HEAD: RESEARCH
SOUTH AFRICAN POLICE SERVICE
PRETORIA
0001

Enquiries/Navrae: Lt Col (Dr) Smit
AC Thenga
Tel: (012) 393 4333
Email: ThengaS@saps.gov.za

APPROVED

LW Mahlatsi
UNIVERSITY OF SOUTH AFRICA

RE: PERMISSION TO CONDUCT RESEARCH IN THE SOUTH AFRICAN POLICE SERVICE: UNIVERSITY OF SOUTH AFRICA: DOCTORATE DEGREE: A CRITICAL REVIEW OF THE IMPLEMENTATION OF THE SECURITY THREAT ASSESSMENT BY A SELECTION OF GOVERNMENT DEPARTMENTS IN GAUTENG: RESEARCHER: LW MAHLATSI

1. The above subject matter refers.

2. You are hereby granted approval for your research study on the above-mentioned topic in terms of National Instruction 4 of 2022.

3. Further arrangements regarding the research study may be made with the following office:

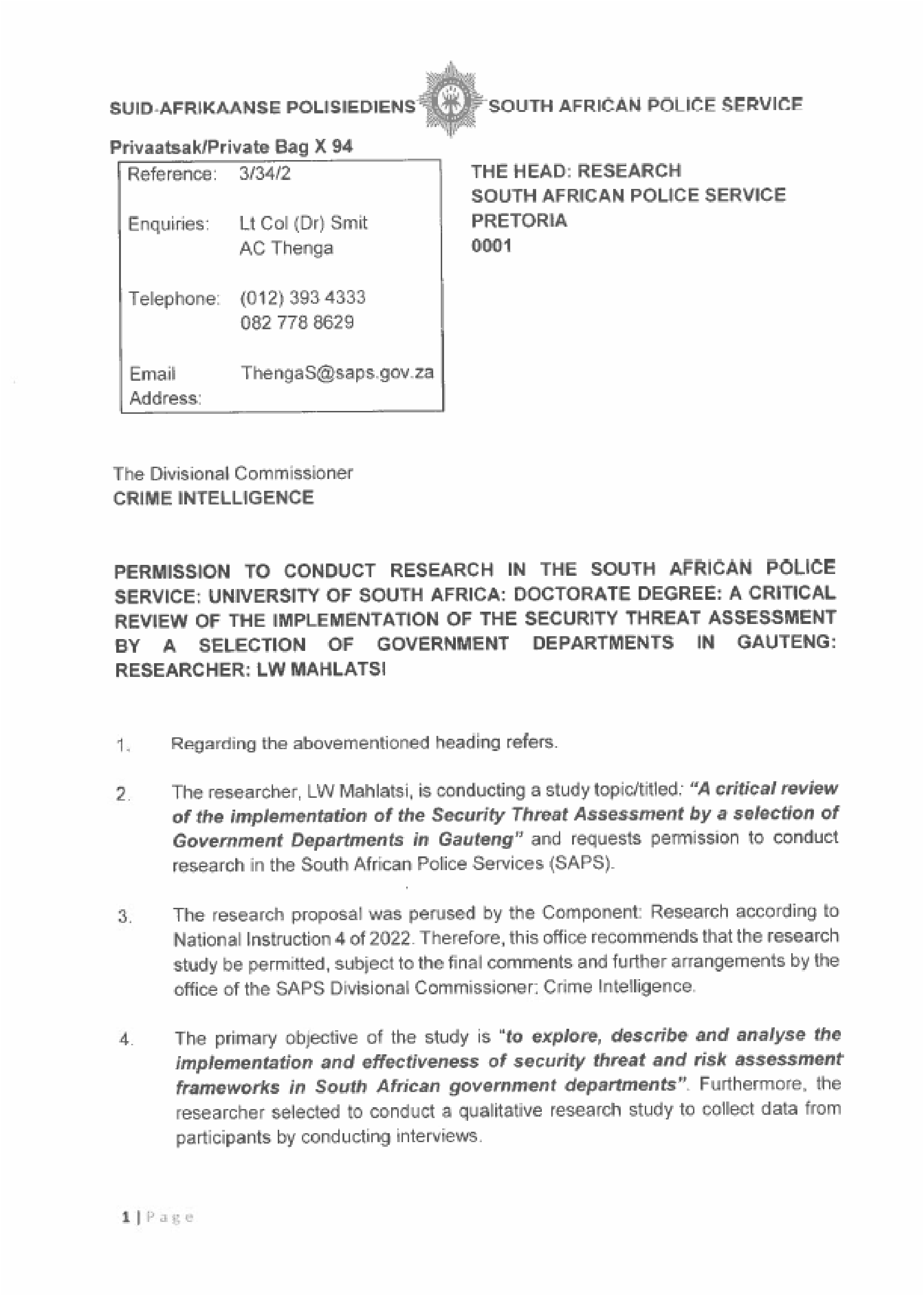
The Divisional Commissioner: Crime Intelligence

- **Contact Person:** Major General Lushaba
- **Contact Details:** (012) 360 1408

4. Kindly adhere to paragraph 8 of our attached letter signed on **2022-08-18** with the same abovementioned reference number.

MAJOR GENERAL
THE HEAD: RESEARCH
DR PR VUMA

Date: 2022 -10- 0 6



SUID-AFRIKAANSE POLISIEDIENS SOUTH AFRICAN POLICE SERVICE

Privaatsak/Private Bag X 94

Reference:	3/34/2
Enquiries:	Lt Col (Dr) Smit AC Thenga
Telephone:	(012) 393 4333 082 778 8629
Email Address:	ThengaS@saps.gov.za

THE HEAD: RESEARCH
SOUTH AFRICAN POLICE SERVICE
PRETORIA
0001

The Divisional Commissioner
CRIME INTELLIGENCE

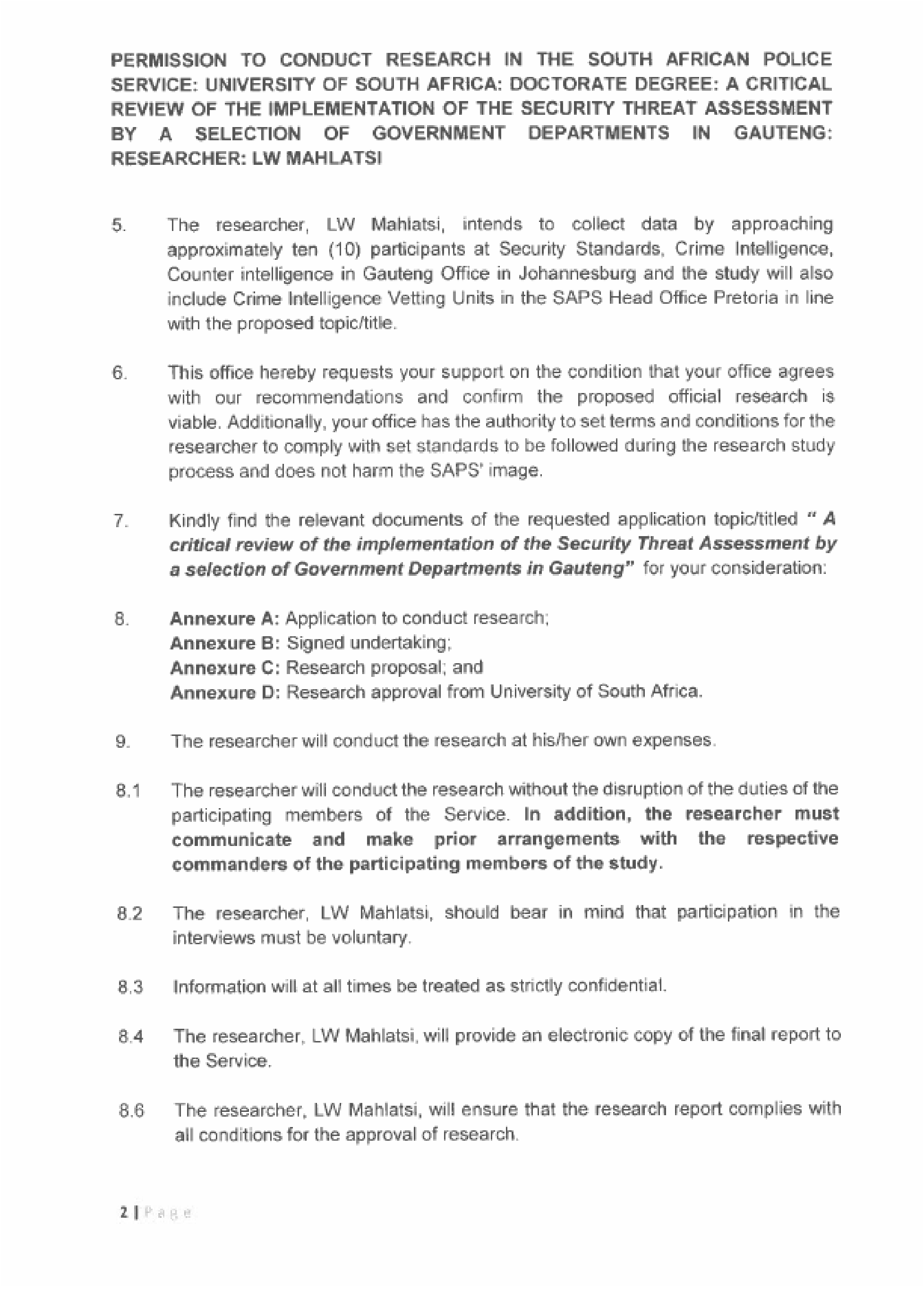
PERMISSION TO CONDUCT RESEARCH IN THE SOUTH AFRICAN POLICE SERVICE: UNIVERSITY OF SOUTH AFRICA: DOCTORATE DEGREE: A CRITICAL REVIEW OF THE IMPLEMENTATION OF THE SECURITY THREAT ASSESSMENT BY A SELECTION OF GOVERNMENT DEPARTMENTS IN GAUTENG: RESEARCHER: LW MAHLATSI

1. Regarding the abovementioned heading refers.

2. The researcher, LW Mahlatsi, is conducting a study topic/titled: ***"A critical review of the implementation of the Security Threat Assessment by a selection of Government Departments in Gauteng"*** and requests permission to conduct research in the South African Police Services (SAPS).

3. The research proposal was perused by the Component: Research according to National Instruction 4 of 2022. Therefore, this office recommends that the research study be permitted, subject to the final comments and further arrangements by the office of the SAPS Divisional Commissioner: Crime Intelligence.

4. The primary objective of the study is "***to explore, describe and analyse the implementation and effectiveness of security threat and risk assessment frameworks in South African government departments"***. Furthermore, the researcher selected to conduct a qualitative research study to collect data from participants by conducting interviews.



PERMISSION TO CONDUCT RESEARCH IN THE SOUTH AFRICAN POLICE SERVICE: UNIVERSITY OF SOUTH AFRICA: DOCTORATE DEGREE: A CRITICAL REVIEW OF THE IMPLEMENTATION OF THE SECURITY THREAT ASSESSMENT BY A SELECTION OF GOVERNMENT DEPARTMENTS IN GAUTENG: RESEARCHER: LW MAHLATSI

5. The researcher, LW Mahlatsi, intends to collect data by approaching approximately ten (10) participants at Security Standards, Crime Intelligence, Counter intelligence in Gauteng Office in Johannesburg and the study will also include Crime Intelligence Vetting Units in the SAPS Head Office Pretoria in line with the proposed topic/title.

6. This office hereby requests your support on the condition that your office agrees with our recommendations and confirm the proposed official research is viable. Additionally, your office has the authority to set terms and conditions for the researcher to comply with set standards to be followed during the research study process and does not harm the SAPS' image.

7. Kindly find the relevant documents of the requested application topic/titled ***" A critical review of the implementation of the Security Threat Assessment by a selection of Government Departments in Gauteng"*** for your consideration:

8. **Annexure A:** Application to conduct research;
Annexure B: Signed undertaking;
Annexure C: Research proposal; and
Annexure D: Research approval from University of South Africa.

9. The researcher will conduct the research at his/her own expenses.

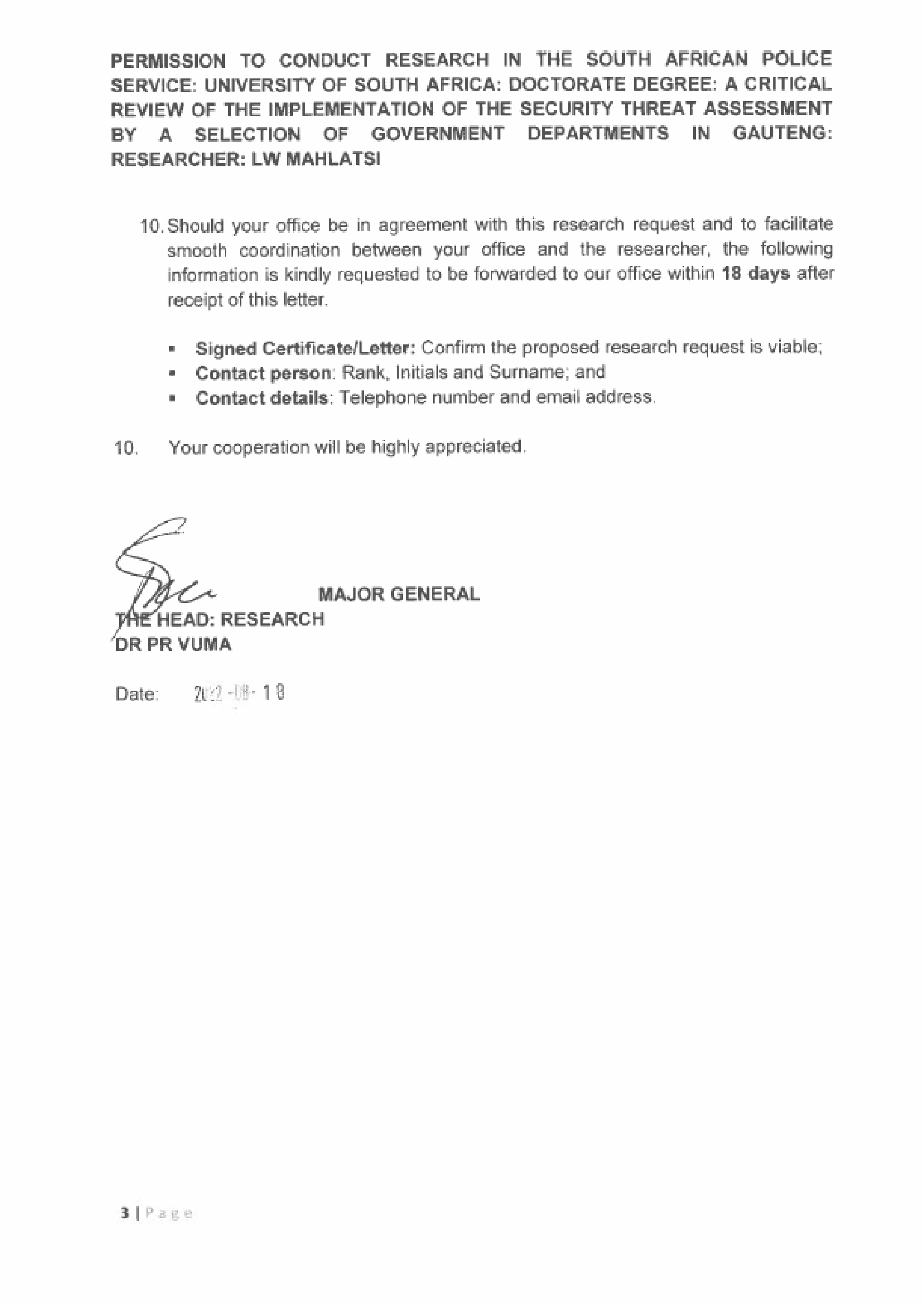
8.1 The researcher will conduct the research without the disruption of the duties of the participating members of the Service. **In addition, the researcher must communicate and make prior arrangements with the respective commanders of the participating members of the study.**

8.2 The researcher, LW Mahlatsi, should bear in mind that participation in the interviews must be voluntary.

8.3 Information will at all times be treated as strictly confidential.

8.4 The researcher, LW Mahlatsi, will provide an electronic copy of the final report to the Service.

8.6 The researcher, LW Mahlatsi, will ensure that the research report complies with all conditions for the approval of research.



PERMISSION TO CONDUCT RESEARCH IN THE SOUTH AFRICAN POLICE SERVICE: UNIVERSITY OF SOUTH AFRICA: DOCTORATE DEGREE: A CRITICAL REVIEW OF THE IMPLEMENTATION OF THE SECURITY THREAT ASSESSMENT BY A SELECTION OF GOVERNMENT DEPARTMENTS IN GAUTENG: RESEARCHER: LW MAHLATSI

10. Should your office be in agreement with this research request and to facilitate smooth coordination between your office and the researcher, the following information is kindly requested to be forwarded to our office within **18 days** after receipt of this letter.

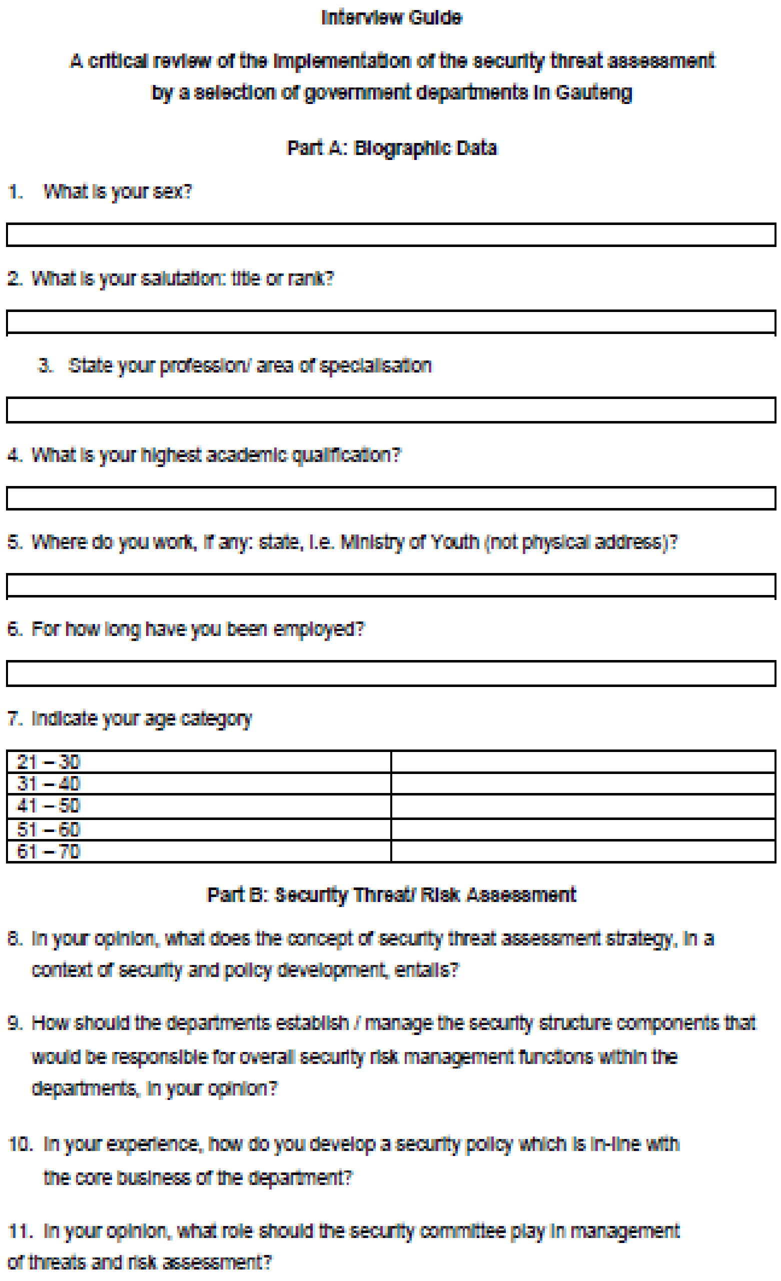
- **Signed Certificate/Letter:** Confirm the proposed research request is viable;
- **Contact person**: Rank, Initials and Surname; and
- **Contact details**: Telephone number and email address.

10. Your cooperation will be highly appreciated.

MAJOR GENERAL
THE HEAD: RESEARCH
DR PR VUMA

Date: 2022 -08- 18

ANNEXURE 6: INTERVIEW GUIDE



Interview Guide

A critical review of the implementation of the security threat assessment by a selection of government departments in Gauteng

Part A: Biographic Data

1. What is your sex?

2. What is your salutation: title or rank?

3. State your profession/ area of specialisation

4. What is your highest academic qualification?

5. Where do you work, if any: state, i.e. Ministry of Youth (not physical address)?

6. For how long have you been employed?

7. Indicate your age category

21 – 30	
31 – 40	
41 – 50	
51 – 60	
61 – 70	

Part B: Security Threat/ Risk Assessment

8. In your opinion, what does the concept of security threat assessment strategy, in a context of security and policy development, entails?

9. How should the departments establish / manage the security structure components that would be responsible for overall security risk management functions within the departments, in your opinion?

10. In your experience, how do you develop a security policy which is in-line with the core business of the department?

11. In your opinion, what role should the security committee play in management of threats and risk assessment?

12. In your view, what strategies, if any, are applied by the departments to detect, combat, and prevent systemic threat and risk in the departments?

13. In your view, what role can the mental care practitioners / employee wellness centre play in the implementation of threat assessment?

14. In your view, what tools can be used to popularize the Minimum Information Security Standard document?

15. If you were to recommend - what actionable strategies would you recommended for purposes of enhancing the implementation of security threat assessment in the government departments?

ANNEXURE 7: EDITOR'S CERTIFICATE

PROOF OF EDITING

I, the undersigned, hereby confirm the academic and language editing, technical compliance, text redaction, and methodological compatibility in respect of the research manuscript of **Mr Lehlohonolo Wonderboy Mahlatsi (Student Number: 43312829),** submitted to me in accordance with the requirements for the Doctor of Literature and Philosophy (D Phil et Litt) in Criminal Justice degree registered with the University of South Africa (UNISA), and entitled:

A critical review of the implementation of the security threat assessment by a selection of government departments in Gauteng

As an independent academic editor, I attest that all possible means have been expended to ensure the final draft of **Mr L.W. Mahlatsis** thesis manuscript coheres with acceptable research methodology practices and language control standards expected of postgraduate research studies at his academic level.

In compliance with expected ethical requirements in research, I have further undertaken to keep all aspects of **Mr L.W. Mahlatsi's** study confidential, and as his own individual initiative.

Sincerely.

T.J. Mkhonto

BA Ed: North-West University, Mafikeng (1985)

MEd: School Administration; University of Massachusetts-at-Boston, USA, Harbor Campus (1987)

DTech: Higher Education Curriculum Policy Reform, Design and Management; University of Johannesburg (2008)

All enquiries:

Email: mkhonto9039@gmail.com
Cell: +27(0)60 401 8279

Signed: ____________________ **Date:** 08 December 2022

Dr T.J. Mkhonto dd/mm/yyyy

Independent Academic Editor

Professional
EDITORS
Guild

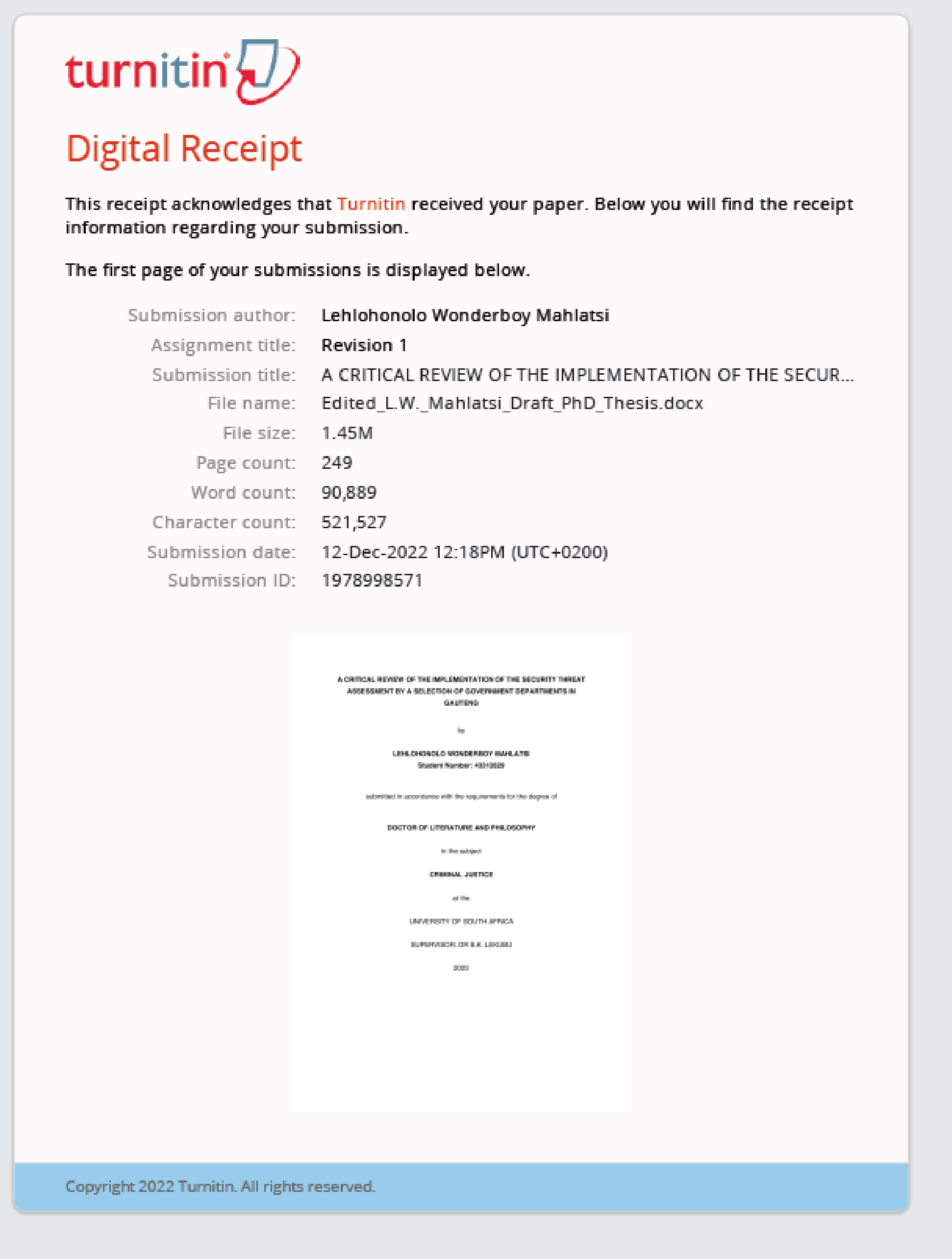
Themba J Mkhonto
Associate Member

Membership number: MKH001
Membership year: February 2022 to March 2023

060 401 8279
mkhonto9039@gmail.com

www.editors.org.za

ANNEXURE 8: TURNITIN DIGITAL RECEIPT



turnitin

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Lehlohonolo Wonderboy Mahlatsi
Assignment title:	Revision 1
Submission title:	A CRITICAL REVIEW OF THE IMPLEMENTATION OF THE SECUR...
File name:	Edited_L.W._Mahlatsi_Draft_PhD_Thesis.docx
File size:	1.45M
Page count:	249
Word count:	90,889
Character count:	521,527
Submission date:	12-Dec-2022 12:18PM (UTC+0200)
Submission ID:	1978998571

A CRITICAL REVIEW OF THE IMPLEMENTATION OF THE SECURITY THREAT ASSESSMENT BY A SELECTION OF GOVERNMENT DEPARTMENTS IN GAUTENG

by

LEHLOHONOLO WONDERBOY MAHLATSI
Student Number: [illegible]

submitted in accordance with the requirements for the degree of

DOCTOR OF LITERATURE AND PHILOSOPHY

in the subject

CRIMINAL JUSTICE

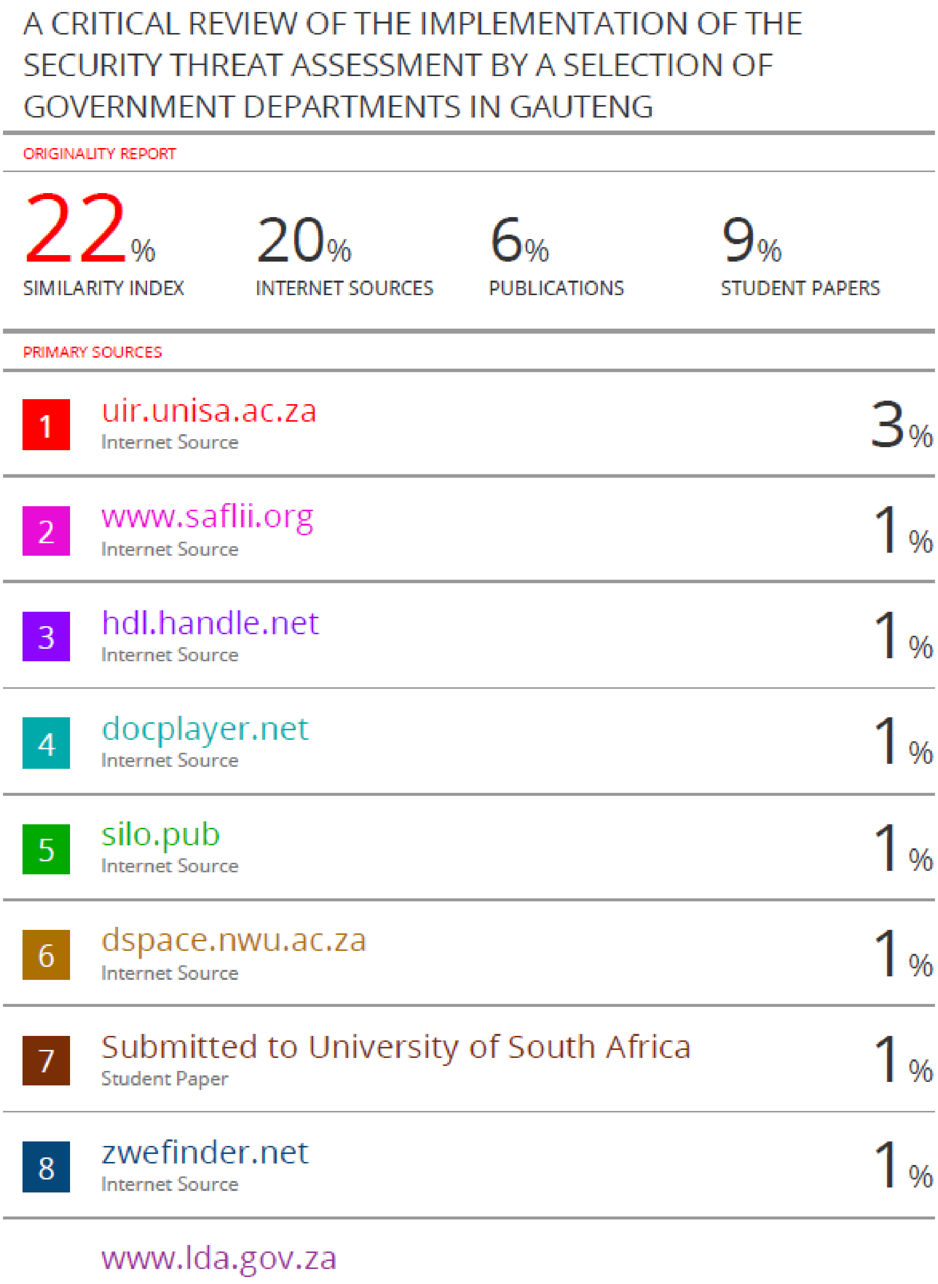
of the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: DR B.K. LEKUBU

2023

ANNEXURE 9: TURNITIN SUMMARY REPORT



A CRITICAL REVIEW OF THE IMPLEMENTATION OF THE SECURITY THREAT ASSESSMENT BY A SELECTION OF GOVERNMENT DEPARTMENTS IN GAUTENG

ORIGINALITY REPORT

22%	20%	6%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	uir.unisa.ac.za Internet Source	3%
2	www.saflii.org Internet Source	1 %
3	hdl.handle.net Internet Source	1 %
4	docplayer.net Internet Source	1 %
5	silo.pub Internet Source	1 %
6	dspace.nwu.ac.za Internet Source	1 %
7	Submitted to University of South Africa Student Paper	1 %
8	zwefinder.net Internet Source	1 %
	www.lda.gov.za	