An Intelligence Risk Management Framework for South Africa: An exploratory perspective

RG Loubser

orcid.org/0000-0003-1135-590X

Dissertation accepted in fulfilment of the requirements for the degree *Master of Arts in Political Studies* at the North-West University

Supervisor: Prof A Duvenhage

Graduation: June 2023

Student number: 26849410

DECLARATION

I declare that - ***An Intelligence Risk Management Framework for SA: An Exploratory Perspective*** to be my work that it has not been previously submitted for any degree or examination purposes at this or any other university and that all the sources used or quoted have been indicated and acknowledged.

Signed Date:28/11/2022

DEDICATION AND ACKNOWLEDGEMENT

I would like to dedicate this dissertation to my wife, Ria, for her patience, support, and belief in me, and for loving me without reservation.

I would like to express my gratitude and appreciation to:

- *Sophôi Theôi—to the immortal, invisible, unique, wise God* who formed me and provides me with the necessary understanding of this uncertain world that we are living in
- My in-laws and family for their support and sacrifices.
- My friends, librarians, and previous colleagues.
- Other intelligence practitioners before me, who did outstanding work - from whom we could learn and be inspired (current serving practitioners and veterans);
- Mr T, for your English proficiency and wisdom.
- My study leader Professor Andre Duvenhage for his guidance and patience over the past years in providing me with leeway to explore this topic.
- For all those, named and unnamed, who provided me with support and assistance during my studies, thank you!

ABSTRACT

Recently, there have been constant reports of natural disasters (e.g. flooding in Kwa-Zulu Natal [KZN] or hailstorms in Alberton, Gauteng), threatening situations ranging from terrorism, ethnic conflicts within states, violent protest action (e.g. 2021 protest in KZN and Gauteng), strikes (e.g. labour strikes in TRANSNET/harbours), and even countries at war (e.g. Ukraine/Russian). Due to international technological development, new threats materialise from e-banking, economic business transfers, identity theft, transnational crime, and cyber-terrorism. By their nature, these risks emerge or come and go. *Some risks diminish or disappear while new risks emerge or come to the fore* (Cleary & Malleret, 2006:44).

An effective national intelligence system is responsible for ensuring that the above threats and risks are adequately attended to, through early warning capabilities and secure systems of communication. While the nature of security challenges and the study of security itself has, in some ways, been transformed by the end of the Cold War, the central task of intelligence services has essentially remained the same. Hulnick (2005:593) observed that: *Nothing is more important in the world of intelligence than preventing surprise*. Thus, an intelligence failure is considered more critical if it comes as a surprise.

Most of these occurrences have resulted in research by academics and practitioners into why these failures or incidents happened and what must be rectified to ensure that no future failures happen. Therefore, this study analyses and assesses intelligence, risk management and national security fields to determine the inter-relationship between these three phenomena and which changes need to be implemented to create an Intelligence Risk Management Framework (IRMF) to overcome some of these shortfalls.

This study described the theories (meta-theories) or processes of intelligence and risk management, which form the foundation on which the IRMF rest. Consequently, in this new threat environment, providing warning (generating secured and actionable knowledge about these challenges) has become considerably more complex, a fact recognised by this study in the SA intelligence context. Thus, an IRMF could contribute to an understanding of threats and provide the required knowledge to make decisions in dealing with them by ensuring a minimum impact on the state and its people.

KEY TERMS: Human Security, Intelligence Failures, Intelligence Risk Management Framework, National Security, Risk Management

OPSOMMING

In Suid-Afrikaanse mediaberiggewing (gepubliseer en elektronies), is daar voortdurend berigte van natuurrampe (bv. oorstromings in KZN, haelstorms in Alberton, Gauteng), dreigende situasies wat wissel van terrorisme, etniese konflikte binne state, geweldadige protesaksies (bv. 2021 protes in KZN en Gauteng), stakings (bv. arbeidstakings in Transnet/hawens en selfs lande in oorlog (bv. Ukraine/Rusland). As gevolg van internasionale tegnologiese ontwikkeling, nuwe bedreigings van kuber, e-bankdienste, ekonomiese besigheidsoordragte, identiteitsdiefstal, transnasionale misdaad en kuberterrorisme realiseer. Vanweë hul aard kom hierdie risiko's na vore en verdwyn dit weer. *Sommige risiko's verminder of verdwyn terwyl nuwe risiko's na vore kom* (Cleary & Malleret, 2006:44)

'n Doeltreffende Nasionale Intelligensiestelsel is direk verantwoordelik om te verseker dat daar voldoende aandag gegee word aan bogenoemde bedreigings en risiko's deur hul vroeë waarskuwingsvermoëns en veilige kommunikasiestelsels. Terwyl die aard van veiligheidsuitdagings en die studie van sekuriteit self op sekere maniere getransformeer is teen die einde van die Koue Oorlog, het die sentrale taak van intelligensiedienste in wese dieselfde gebly. 'n Geleerde van Intelligensiestudies noem in 'n onlangse artikel: *Daar is niks belangriker in die wȇreld van intelligensie as die voorkoming van verrassings nie* (Hulnick, 2005:593). 'n Intelligensie mislukking word as meer kritiek beskou as dit as 'n verrassing kom.

Die meeste van hierdie voorvalle het aanleiding gegee tot navorsing deur akademici en praktisyns om te bepaal waarom hierdie voorvalle gebeur het, asook wat reggestel moet word om te verseker dat soortgelyke toekomstige voorvalle verhoed word. Die studie ontleed en analiseer die intelligensie, risikobestuur en nasionale veiligheidsvelde om die onderlinge verband tussen hierdie drie verskynsels te bepaal en watter wysigings geimplementeer moet word ten einde 'n Intelligensie Risikobestuur Raamwerk te ontwikkel om hierdie tekortkominge te oorkom.

Hierdie studie sal die teorieë (metateorieë) of prosesse van Intelligensie en Risikobestuur beskryf wat die grondslag vorm waarop 'n Intelligensie Risikobestuur Raamwerk ontwikkel sal word. Gevolglik, in hierdie nuwe omgewing van bedreigings, het die verskaffing van waarskuwings (generering van veilige en uitvoerbare kennis van hierdie uitdagings) aansienlik meer ingewikkeld geword, 'n feit wat deur hierdie studie erken word in die Suid-Afrikaanse Intelligensie konteks. 'n Intelligensie Risikobestuur Raamwerk kan bydra tot 'n begrip van bedreigings en die nodige kennis verskaf om besluite te neem om die hantering daarvan te verseker met die minimum impak op die staat en sy mense.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

ANC	African National Congress
AG	Auditor-General
BRICS	An acronym for five leading emerging economies: Brazil, Russia, India, China, and South Africa
CCSI	Cabinet Committee on Security and Intelligence
CIVETS	An investing acronym for the countries of Colombia, Indonesia, Vietnam, Egypt, Turkey, and South Africa
CGE	Commission for Gender Equality
CODESA	Convention for a Democratic South Africa
COPE	Congress of the People
CRL Rights Commission	Commission for the Promotion and Protection of the Rights of Cult Religious and Linguistic Communities
DA	Democratic Alliance
DCAF	Democratic Control of Armed Forces
DG	Director-General
HDI	Human Development Index
DI	Defence Intelligence
DSO	Directorate of Special Operations or known as the 'Scorpions'
EFF	Economic Freedom Fighters
ERM	Enterprise Risk Management
FATF	Financial Action Task Force
GCDCAF	Geneva Centre for the Democratic Control of Armed Forces
GDP	Gross Domestic Profit
GILAA	General Intelligence Laws Amendment Act No. 11 of 2013
GNI	Gross National Income
GNU	Government of National Unity
GPRI	Global Political Risk Index
HDI	Human Development Index
HLRP	High-Level Review Panel
IBSA	A unique Forum: India, Brazil and South Africa
IC	Intelligence Community
IEC	International Electro-Technical Commission
IFP	Inkatha Freedom Party
IFRM	Institute of Risk Managers
IG	Inspector-General
IIAG	Ibrahim Index of African Governance

IJR	Institute for Justice and Reconciliation
IMF	International Monetary Fund
IRM	Intelligence Risk Management
IRMF	Intelligence Risk Management Framework
IRR	Institute of Race Relations
ISAC	Information Sharing and Analysis Centre
ISO	International Organisation for Standardisation
ISS	Institute for Security Studies
IWGNS	International Working Group on National Security
JSCI	Joint Standing Committee on Intelligence
KZN	Kwa-Zulu Natal
LGE	Local Government Election
NC	National Communication
NDP	National Development Plan
NIA	National Intelligence Agency
NICOC	National Intelligence Coordinating Committee
NIS	National Intelligence Service
NPA	National Prosecution Authority
NSC	National Security Council
NSS	National Security Strategy
NUM	National Union of Mineworkers
OALD	Oxford Advanced Learner's Dictionary, 8th edition
ODNI	Office of the Director of National Intelligence
OED	The Shorter Oxford English Dictionary
OIGI	Office of the Inspector-General of Intelligence
ORM	Operational Risk Management
PAGAD	People Against Gangsterism and Drugs
PFMA	Public Finance Management Act 1 of 1999
PPP	Public-Private Partnerships
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act
RM	Risk Management
RSA	Republic of South Africa
SA	South Africa
SADC	Southern African Development Community
SAHRC	South African Human Rights Commission
SANAI	South African National Academy for Intelligence

SANDF	South African National Defence Force
SASS	South African Secret Service
SAPS	South African Police Service
SARIMA	South African Risk and Insurance Management Association
SCOPA	Standing Committee on Public Accounts
SO	Special Operations
SOE	State-Owned Entity
SSA	State Security Agency
TEC	Transitional Executive Council
TICI	Transparency International Corruption Index
UK	United Kingdom
UNISA	University of South Africa
UNSTT	Unit Nations System Task Team
USA	United States of America
WB	World Bank
WEF	World Economic Forum
WWII	World War II

CHAPTER 1: INTRODUCTION, PROBLEM STATEMENT AND METHODOLOGIES

Risk management is one of those ideas that a logical, consistent, and disciplined approach to the future's uncertainties will allow us to live more prudently and productively, avoiding unnecessary waste of resources. Kloman (2010:21)

1.1 Background and Motivation

In the past hundred years, there have been constant reports of natural disasters, and threatening situations ranging from terrorism, ethnic conflicts within states, violent labour action, strikes, and even countries at war. Due to international technological development, new threats materialise from e-banking, economic business transfers, identity theft, transnational crime, and cyber-terrorism. By their nature, these risks come and go. According to Cleary and Malleret (2006:44), *Some risks diminish or disappear while new risks emerge or come to the fore*. They furthermore believe that *Some of these threats and risks that we are faced with are old. New manifestations, however, need to be handled in such a way that the two facets of risk are properly addressed, namely the potential threat and the opportunity associated with it* (Cleary & Malleret, 2006:44).

An effective national intelligence system is responsible for ensuring that the above risks are adequately attended to through their early warning capabilities and secure systems of communication. The South African (SA) White Paper on Intelligence (1995:2) (hereafter referred to as 'the White *Paper*') describes the purpose of intelligence as follows: *in the modern, post-Cold War world, for intelligence to be relevant, it must serve the following purposes:*

- *to provide the policymakers, with timeous, critical, and sometimes unique information to warn them of potential risks and dangers. This allows the policymakers to face the unknown and best reduce their uncertainty when critical decisions have to be made;*
- *to identify opportunities in the international environment by assessing actual or potential competitors' intentions and capabilities. This competition may involve the political, military, technological, scientific, and economic spheres, particularly the field of trade; and*
- *to assist good governance by providing natural critical intelligence that highlights the weaknesses and errors of government. As guardians of peace, democracy, and the constitution, intelligence services should tell the government what they ought to know and not what they want to know*.

While the nature of security challenges and the study of security itself has, in some ways, been transformed by the end of the Cold War, the central task of intelligence services has essentially remained the same. Hulnick (2005:593) observed that *Nothing is more important in the world of*

intelligence than preventing surprise. By implication, an intelligence failure is considered more critical if it comes as a surprise. Examples of this are the attack on Pearl Harbour, the coordinated Egyptian-Syrian attack against Israel on Yom Kippur, the invasion of Afghanistan by Soviet forces, the attacks of 11 September 2001 in the United States of America (USA), and the most recent incidents of terrorism in France, United Kingdom (UK), Africa, Mali, and the Middle East. These examples are just some of the surprises that have been attributed to intelligence failures (Bar-Joseph and Kruglanski, 2003; Halberstam, 2007; Maceachin, 2003; Wohlstetter, 1962; 9/11 Commission, 2004).

Most of these attacks have resulted in a series of research by academics and practitioners into why these failures occurred and what must be rectified to ensure that no failures of this nature happen in the future. The research results indicate that surprises can be prevented by adequate or 'better' warnings (Lowenthal, 2009; Parker, 2007). A warning is considered to play the classic strategic intelligence role (McCarthy, 1994); thus, it was the principal impetus for the creation of the new dispensation in SA and new roles and functions for SA's intelligence agencies in 1995 in so far as the control of strategic warning and foreknowledge was concerned.

The above-said understanding of the foundation of the function of intelligence is needed to provide professional and timeous warnings and strategic direction. Therefore, this study will describe the theories or processes of intelligence and RM that form the foundation on which an Intelligence Risk Management Framework (IRMF) will rest and be developed. Such a foundation and RM framework, from which an intelligence threat or risk assessment operates, should be developed. In other words, intelligence services are tasked with monitoring threats to their country's national security interests that are more diverse, interconnected, and dynamic than ever before. Consequently, in this new environment, the task of providing warnings (in the sense of generating secured and actionable knowledge about these challenges) has become considerably more complex, a fact recognised by this study in the SA intelligence context. Thus, an IRMF could contribute to an understanding of threats and provide the required knowledge to make decisions in dealing with these threats. Intelligence needs to start taking cognisance of other academic fields within Social Studies to obtain better-structured tools and models to ensure improved early warning on strategic surprises.

This study concurs with Bracken, Bremmer and Gordon (2008:1), who argue that *the emergence of RM as a distinctive field of study should influence intelligence analysis in intelligence work*. They add that RM also has influenced other fields of study, such as *finance, business, engineering, the security industry, environmental protection, and epidemiology*, to name a few (Bracken *et al.*, 2008). This study, therefore, aims to conceptualise and develop an IRMF to ensure better early warnings in the SA intelligence context with these aspects in mind.

1.2 Problem Statement

Intelligence remains a vital tool – albeit secret – to assist the state in attaining its goals to secure, protect and deliver a good life for all. This argument is supported by Born and Leigh (2007:4), as well as Caparini (2007b:1), who states that *Intelligence and security services are key components of any state, providing independent analysis of information relevant to the external and internal security of state and society and the protection of vital national interests*. Due to the complexity of the global environment we live in, the intelligence regime needs to make changes to handle threats and risks more systematically by using Social Science tools such as RM. This raises the question of how an IRMF and/or assessment module(s) (according to this study) should be developed and conceptualised within an intelligence framework. Intelligence and RM are both viewed as art forms and dynamic sciences that deliver a destined outcome to enhance the governance of a country, institution, or organisation. Thus, to understand and define both the environments of intelligence and RM, one needs to go back to the root theories of these concepts to clarify and describe their inter-relationship and how these concepts can support each other in a specific framework, as can be seen in the sub-sections below.

1.2.1 Enhancing intelligence and RM collaboration

The historical development of RM, which means different things to different people, came from the same intellectual roots as the specialised fields it is used in today. RM found its origin in the USA in the late 1950s and was founded in statistical methods (1920s and 1930s) and mathematical concepts in the military, called operations research (decision sciences) (Bracken et al, 2008:3-4). Bracken et al (2008:3-4) argues that *stated simply, risk out of these developments is defined as the product of two things: likelihood and consequences (Impact)*. When discussed, one needs to look at the management of these two concepts to understand RM in its full context. The different views regarding risk and uncertainty complicate this subject because of how it is perceived. Therefore, the study will show that using an RM framework in the intelligence environment (analysis) can provide more structure and improve management and processes to understand its dynamics. This will ensure that intelligence provides timeous early warning and foreknowledge services.

Furthermore, a political regime may influence intelligence. As Caparini (2007b:1) explains, intelligence services/agencies are one of the essential governance functions of any state to *provide independent analysis of information relevant to the external and internal security of the state and society and protection of vital national interests*. These concepts and functions of intelligence were also reflected by one of the oldest ‘traditional’ views, which is found in a Chinese classic entitled *The Art of War,* attributed to a sixth-century B.C. general and military thinker named Sun Tzu (Sun Tzu, The Art of

War, as in Griffith, 1963:144-45). Therefore, the study will show that through an IRMF, these central functions can be structured and managed to ensure a professional intelligence product of early warning and foreknowledge. As a Social Science tool, RM will enhance intelligence as it develops other fields, such as finance and engineering.

Additionally, the importance of politics' influence on the functioning of intelligence is evident in the structuring and management of intelligence agencies, as well as how the intelligence regime reports/communicates early warnings, foreknowledge and surprises to policy-makers. Therefore, the structuring, management, politicisation of intelligence and the instability of the structures due to poor management decisions will influence the use of RM as a Social Science tool to enhance intelligence analysis processes. These aspects are also crucial in the SA context to determine the current status of governance in SA and what influence the government/state has on good governance.

1.2.2 Intelligence processes, Intelligence Risk Management Framework and national security defined

This section will investigate and analyse the three phenomena to determine the relationship between them in an effort to demarcate the field and design a conceptual framework of key constructs and concepts in the IRM domain.

1.2.2.1 Intelligence process

This study must also conceptualise what intelligence is and means. Despite the efforts to formulate intelligence theories, it is complicated to define intelligence as it has different meanings for different people (Rand, 2005:2). Most definitions of intelligence are based on Kent's (1949:vii) description: *the knowledge which our highly placed civilian and military men must have to safeguard the national welfare*. In addition, Kent (1949:ix) refers to the three 'distinct things' intelligence practitioners refer to when they use the word intelligence, namely:

- Knowledge – finished intelligence product;
- Organisation – way in which intelligence services are organised; and
- Activity – way intelligence services collect and analyse information.

Against this background, it is essential to note that intelligence is a dynamic science and changes together with its environment. In this regard, the focus of intelligence has changed since the end of the Cold War in 1989. During the Cold War, intelligence was principally geared towards the military and the struggle between East-West ideological and military rivalry between the USA and the Soviet Union (Johnson, 1999:6; Sheehan, 2000:329; Treverton, 2003:11). Countries aligned themselves

along this line and focused their security priorities accordingly (Johnson, 1999:6; Sheehan, 2000:329; Treverton, 2003:1). After the end of the Cold War, the security focus changed, and due to the borderless environment, the enemy is no longer state-bound. The focus has moved to issues such as the proliferation of weapons, growth of ethnic nationalism and extremism, international terrorism, and transnational crimes (Johnson, 1999:5). National security is no longer limited to a country's borders but towards a common global advisory.

Similarly, SA intelligence also experienced a significant change after the end of apartheid in 1994. In the SA context, the focus of intelligence during apartheid was on the African National Congress's (ANC) liberation movement (O'Brien, 2011:10). After 1994, the focus of national security shifted to a broader range of threats related to both the SA state and society (O'Brien, 2011:10). The White Paper (1995) and the Constitution of the Republic of South Africa (1996) (hereafter 'the Constitution') form the backbone of the new approach to security in general and intelligence in particular.

To summarise the understanding of the role, functions, and restructuring of intelligence in the SA context (with proper control and oversight), this study postulates the use of Social Science tools by intelligence agencies, to enhance their capability and provide timeous warning and foreknowledge to ensure democratic governance. Furthermore, this study seeks to analyse and determine if a more structured approach to intelligence risk threat analysis will have the necessary impact to ensure that the intelligence regimes can enhance the governance processes, which will direct the political regime to withstand the severity of global threats and risks.

1.2.2.2 Intelligence Risk Management Framework

A conceptualised IRMF will enhance intelligence analysis, management of intelligence processes, and the quality of intelligence products. It will further enhance and give more structure to the intelligence analysis processes, which some academics currently question (Clark, 2013; Hulnick, 2006; Johnson, 2003; 2009; Lowenthal, 2009). Furthermore, Mabey, Gulledge, Finel and Silverthorne (2011:10) argue that *Implementing an explicit IRMF is not a solution that can eliminate the political influence on intelligence early warning or foreknowledge, either within or between countries. However, it does provide tools to make the consequences of choices clearer to decision-makers and can help create a common framework of understanding between different actors which itself should help promote agreement and greater cooperation regarding intelligence.*

1.2.2.3 National Security

For this study, national security is defined broadly, taking its cue from the International Working Group on National Security (IWGNS) (2013:3). The group, which consists of experts from both developed and developing countries, regard *National security is the first and most important obligation of government. It involves not just the safety and security of the country and its citizens. It is a matter of guarding national values and interests against both internal and external dangers – threats that can potentially undermine the security of the state, society and citizens. It must include not just freedom from undue fear of attack against their person, communities or sources of their prosperity and sovereignty, but also the preservation of the political, economic and social values – respect for the rule of law, democracy, human rights, a market economy and the environment – which are central to the quality of life in a modern state.*

This said, the Constitution itself upholds these views: *national security must reflect the resolve of SA citizens, as individuals and as a nation, to live as equals, to live in peace and harmony to be free from fear and want … 'a classic expression of human security'* (RSA, 1996: s 198). Therefore, this dissertation focuses on an IRMF as a Social Science tool that can enhance intelligence processes to deliver intelligence products that will enhance national security and ensure good governance.

1.2.2.4 The Benefits of a Risk Management approach

RM as Social Science tool is applied in different fields with success. Therefore, it has been argued that the conceptualising and implementation of an IRMF would also enable SA to enhance its democracy and develop its economy to benefit all within its society. According to Mabey *et al.* (2011:10), *RM is a practical process that provides a basis for decision-makers to compare different policy choices. It considers the likely human and financial costs and benefits of investing in prevention, adaptation, and contingency planning responses. Some risks are not cost-effective to try and reduce, just as there are some potential impacts to which we cannot feasibly adapt while retaining current levels of development and security. RM approaches do not provide absolute answers but depend on specific decision-makers' values, interests, and perceptions. RM is as much about managing risk as it is about the scientific measurement of risk itself. It has often taken a decade or more of intense debate for robust RM strategies to emerge to tackle existing national security issues.*

1.3 Research Aim, Questions and Objectives of this Study

Considering the research topic and this study's problem statement, the following primary question is submitted and explored throughout the study: *How can an RM framework be developed and used in*

intelligence processes within a state as an essential Social Science tool to advise the policy-maker/client on potential threats, risks, vulnerabilities and opportunities? Contributing to the solution of this primary research question are several secondary questions that must be explored and answered by the study:

- How are risks and uncertainty theory understood within intelligence, RM, and the national security context?
- What would constitute an analytical framework for Intelligence Risk Management (IRM) within the statutory intelligence environment?
- What are the historical and current developments and applications of the IRM field of study?
- What would the contribution and benefits be of an IRMF for SA?

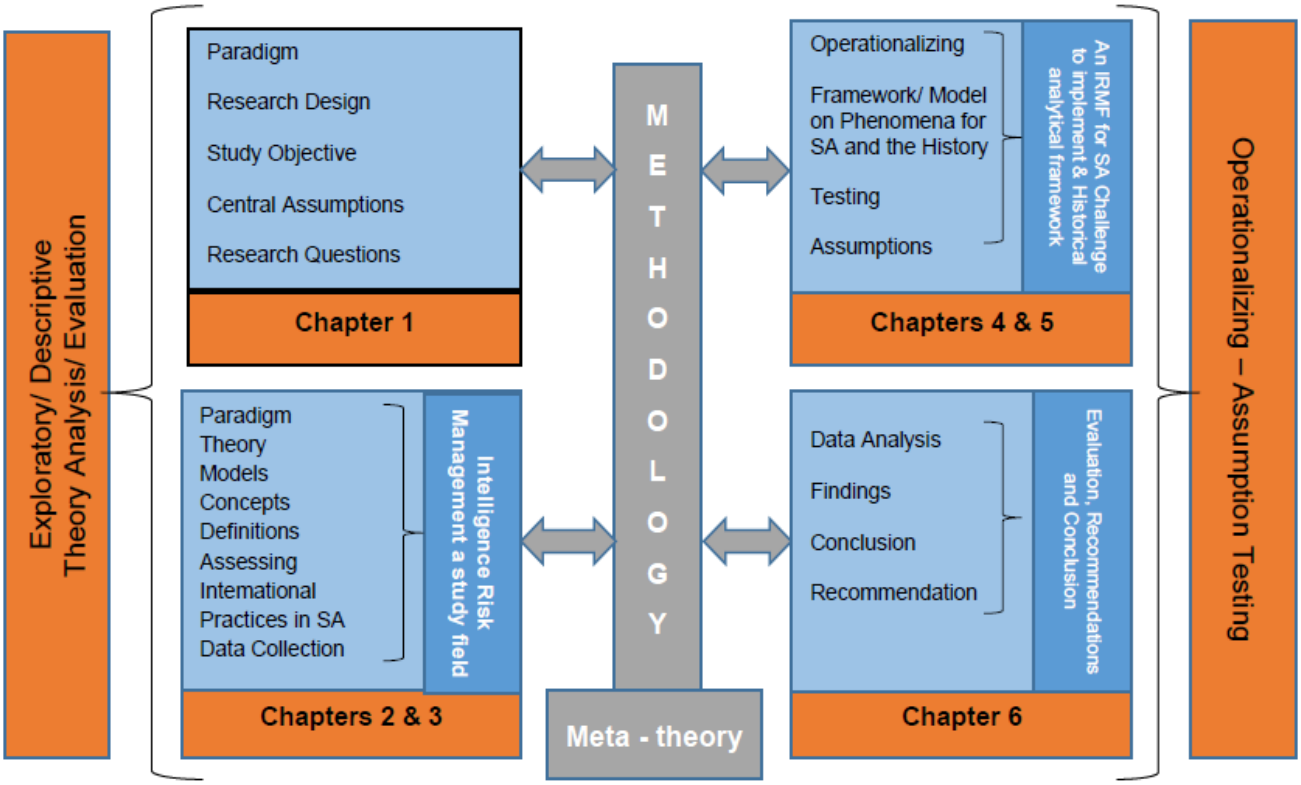
The core aim of this study was to investigate a new field of study, namely IRM, which will contribute to intelligence studies. Therefore, the study has identified the following primary research objective to address the research study: *Develop an IRMF which can enhance the intelligence processes to deliver intelligence products that can enhance national security and good governance in a more structural and controlled manner*. The implementation of the study was evaluated against the SA environment, and case studies will be used to demonstrate the use of IRMF in the practical intelligence environment. Furthermore, the following secondary objectives were attained to provide a more precise contextualised and systematic overview of the SA context:

- Through explorative investigation and analysis, the author will define and describe the theories influencing the study to address the inter-relationship between intelligence, uncertainty, risk, and national security in an IRM field of study.
- Conceptualise and construct an IRMF.
- Describe and explain the historical development and application of IRM in the SA context.
- Assess and evaluate the application of an IRMF for SA and its enhancement of national security.

1.4 Research design

The study explored and evaluated RM frameworks and intelligence risk threat assessment modules to advise which of these frameworks and modules will benefit the intelligence regime to enhance national security and good governance. A mainly explorative and qualitative research methodology was used in this study. Maree (2011:51) describes qualitative research as a *research methodology concerned with understanding the processes and the social and cultural context which underlies various behavioural patterns and is mostly concerned with exploring the 'why' questions of research*. The study further established, through deductive reasoning, an RM framework and techniques/methods, which can enhance the intelligence risk analysis process to provide timely forewarning and strategic threat intelligence to the policy-maker/client. Although this study, as referred

to in the title – mainly focuses on an explorative perspective approach, it also implements explanatory and descriptive research approaches. This study applied a meta-theoretical and theoretical approach to analyse the different interdisciplinary concepts and theories applicable to this research topic. Figure 1 below depicts the study's research framework.



Source: Researcher's construct

Figure 1: Research framework

1.5 Methodology

The dissertation will focus on an IRMF, which has not yet been studied in detail as a field of study. Some studies indicate that RM should be used to enhance intelligence processes and specifically the intelligence analysis function. Therefore, the research study will explore, describe and explain the intelligence and RM phenomena through comparative and descriptive research methods. During the literature and data study, primarily open-source/overt information (books, journals, Internet, and articles) will be used to ensure that the dissertation is available and not classified due to the secret nature of the intelligence environment.

The dissertation unfolded its methodological approaches in several ways. Chapter One explores the literature and data available on the three prominent phenomena in the study (intelligence, RM, and national security), and a proposal on how this dissertation will investigate the research study is provided. Chapter Two defined and explained the definitions, concepts, functions, and purposes of

intelligence, RM, and national security through conceptualisation and theoretical analysis. The most critical understanding or knowledge regarding the three phenomena' inter-relation/interaction/work will be explained, influencing the developed framework in Chapter Three. Furthermore, Chapter Three explored all relevant intelligence and RM frameworks to conceptualise and develop an IRMF for the SA environment. Chapter Four used exploratory and historical research methods to explain, describe and evaluate the development and implementation of SA. This research will ensure that most of the problems and shortcomings in the SA intelligence environment are identified, and recommendations to enhance these aspects will be explained and assessed. In Chapter Five, a case study was conceptualised and developed to analyse the current instability of the SA. The reasons for the instability will be better understood, and plausible scenarios will be formulated from this analysis of SA. The final chapter (Chapter Six) examined whether the research objectives have been reached and if the research questions were sufficiently answered. It will also make proposals for further studies on the topic of intelligence studies as a field of study.

1.6 Literature study

One of the primary methodologies within qualitative research is a literature review. The literature that was used in this study are shown in the table below.

Table 1: Literature Study

LITERATURE STUDY LIST		
THEME	**AUTHOR**	**TITLE**
RM Domain	Bernstein (1996)	*Against the Gods (The remarkable story of risk)*
	Covello & Mumpower (1985)	*Risk Analysis and Risk Management: An Historical Perspective*
	Hand (2014)	*The Improbability Principle*
	Knight (1921)	*Risk, Uncertainty and Profit*
	Quiggin (2007)	*Seeing The Invisible (National Security Intelligence in An Uncertain Age)*
	Taleb (2010)	*The Black Swan (The Impact of The Highly Improbable)*
RM as a Social Science Tool	Blunden & Thirlwell (2013)	*Mastering Operational Risk*
	Bracken, *et al.* (2008)	*Managing Strategic Surprise (Lessons from Risk Management and Risk Assessment)*
	Damodara (2007)	*Strategic Risk Taking: A Framework for Risk Management*
	Gill & Phythian (2012)	*Intelligence in an Insecure World*
	International Organisation for Standardisation (ISO)	*ISO 31000: 2009*
	ISO	*ISO/IEC Guide: 73/2009*
	Cleary & Malleret (2006)	*Resilience to Risk*
	Shulsky & Schmitt (2002)	*Silent Warfare: Understanding the World of Intelligence*
	Valsamakis, Vivian & du Toit (2005; 2010)	*Risk Management – managing enterprise risks*
	Walsh (2014)	*Building Better Intelligence Frameworks Through Effective Governance*
	Young (2008)	*Operational Risk Management (ORM) Third Impression*
Intelligence Theory	Cavelty & Mauer (2009)	*Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence*
	Gill *et al.* (2009)	*Key questions and debates*
	Johnson (2003)	*Sketches for a theory of strategic intelligence*
	Kahn (2001)	*A historical theory of intelligence*

LITERATURE STUDY LIST		
THEME	**AUTHOR**	**TITLE**
	Kent (1966)	*Strategic intelligence for American world policy*
	Rand (2006)	*Towards a theory of intelligence (Conference report)*
	Rathmell (2002)	*Towards postmodern intelligence*
	Scott & Jackson (2004)	*The Study of Intelligence in Theory and in Practice*
	Sims (2009)	*Defending Adaptive Realism: Intelligence Theory Comes of Age*
Intelligence Define, Describe, Elements and Functions	Gill & Phythian (2006)	*Intelligence in an insecure world*
	Johnson & Wirtz (2008)	*Intelligence and National Security: The Secret World of Spies*
	Kent (1966)	*Strategic intelligence for American world policy*
	Lowenthal (2006 & 2009)	*Intelligence from secrets to policies*
	Shulsky (2009)	*What is intelligence? Secrets and Competition Among States*
	Shulsky & Schmitt (2002)	*Silent warfare: understanding the world of intelligence*
	Sims (2009)	*What is Intelligence? Information for Decision-Makers*
	Sun Tzu (Translated by Cleary) (2005)	*The Art of War*
	Treverton (2003)	*Reshaping National Intelligence for an Age of Information.*
National Security	Cawthra (2013)	*National Security and the right to information: the case of South Africa*
	Cronje (2014, 2017)	*A Time Traveller's Guide and Cronje*
	Cronje (2020)	*The Rise or Fall of South Africa*
	Fingar (2011)	*Reducing Uncertainty - Intelligence Analysis and National Security*
	Hough (2006)	*The Concept of a National Security Strategy: The case of the United States and South Africa*
	Hough (2013)	*Understanding Global Security*
	IWGNS: (2013)	*International Working Group on National Security: Define National Security (Democratic Control of Armed Forces - DCAF)*
Intelligence within the SA Context	(Act 108 of 1996)	*The Constitution of the Republic of SA*
	(Act 25 of 2002)	*Electronic Communications and Transactions Act 25*
	(Act 2013) (Act 66 of 2000)	*The General Intelligence Laws Amendment Act (GILAA)*
	(Act 65 of 2002)	*Intelligence Services Act 65*
	(Act 66 of 2002 amended)	*Intelligence Services Control Act 42*
	(Act 39 of 1994)	*The National Strategic Intelligence Act*
	(Act 70 of 2002)	*The Regulation of Interception of Communications and Provision of Communication-related Information Act 70*
	Africa (2012)	*The policy evolution of the SA intelligence evolution*
	Africa (DCAF, 2011)	*The Transformation of the South African Security Sector: Lessons and Challenges*
	High-Level Review Panel (HLRP) (2018)	*The State Security Agency*
	Ministerial Review Commission on Intelligence (2008)	*Intelligence in A Constitutional Democracy*
	O'Brien (2011)	*The SA intelligence services*
	South African Institute of Race Relations (IRR), (2016)	*Life in South Africa: Reasons for Hope*
	Van den Berg (2014)	*Master's Dissertation: The Intelligence Regime in SA (1994-2014): An Analytical perspective*
	White Paper (1995)	*The White* Paper *on Intelligence*
Analyse and Understand Political Systems	*Fukuyama (2010)*	*The Origins of Political Order*
	Machiavelli (1532 repr. n.d.)	*The Prince*
	Schwartz: (1996)	*The art of the long view: paths to strategic insight for yourself and your company*
	Van der Heijden (2005)	*The Art of Strategic Conversation*
	DCAF (03/2006)	*Backgrounders Series: Contemporary Challenges for the Intelligence Community (IC)*

LITERATURE STUDY LIST		
THEME	**AUTHOR**	**TITLE**
Democratic Principles for Intelligence and Security Sectors	DCAF (2015)	*Backgrounders Series: The Justice Sector, Roles, and responsibilities in good security sector governance*
	DCAF (2015/SS)	*Backgrounders Series: The Security Sector*
	DCAF (2015)	*Backgrounders Series: Parliaments*
	DCAF (2017)	*Backgrounders Series: Intelligence Oversight*
	DCAF (2010)	*Backgrounders Series: National Security Councils*
Social Science Research	Bhattacherjee (2012)	*Social Science Research: Principles, Methods, and Practices*
	Maree (2007)	*First Steps in Research*
	Ritzer (2001)	*Explorations in Social Theory - From Meta-theorising to Rationalisation*
	Siu (2009)	*A Meta-Theory of Risk: Risk as Reflexive, Social Learning*
	Zinn (2008)	*Social Theories of Risk and Uncertainty*
Statistical Data	British Bankers Association	*Gold database*
	IIAG (2022)	*The Ibrahim Index of African Governance (IIAG)*
	International Monetary Fund (IMF) (2006-2020)	*Country Report South Africa*
	Institute for Justice and Reconciliation (IJR) (2022)	*Afrobarometer (2022)*
	IJR (2021)	*Reconciliation Barometer, 2021*
	OECD (2015)	*Principles of Corporate Governance*
	Pew Research Centre, 2019	*In South Africa, Racial Divisions and Pessimism About Democracy Loom Over Elections*
	Schwella *et al.* (2017):	*South African Governance*
	Statistics South Africa (StatsSA) (2021).	*Statistics South Africa - Economic Growth*
	TICI (2022)	*Transparency International Corruption Index - Office in SA: Corruption Watch*
	Unit Nations System Task Team (UNSTT) (2012)	*Governance and Development*
	World Economic Forum (WEF), (2022)	*World Risk Report*
	World Bank (WB) (2018)	*South Africa Economic Update - Jobs and Inequality*

Source: Researcher's construct

1.7 Chapter Division

The study was divided into six chapters. They are as follows:

Chapter One: Introduction, Problem Statement and Methodology: Chapter One introduces the study. In this chapter, a brief overview of the structure of the study is provided, as well as its objectives and methods. RM, intelligence, and national security are contextualised from which a problem statement, research questions, and research objectives are derived. The methodology used to achieve the goals is discussed before a brief outline is given regarding the study's contribution. The introductory chapter concludes by specifying the chapter division and briefly discussing the content of each chapter.

Chapter Two: Intelligence RM a Study Field – Meta-theoretical Perspectives and Points of Departure: This chapter will address the demarcation of IRM as a study field. It furthermore explores and examines the development, tradition/paradigm, and typology of theory in the meta-context.

Chapter Three: An Intelligence RM Framework: Chapter Three describes and explains the different theories which influence and form the framework. In addition, this chapter selects and motivates a theoretical point of departure for the development of an IRMF, which will influence and enhance intelligence analysis.

Chapter Four: Intelligence RM in the SA context - Implementing the IRMF: This chapter aims to contextualise the security and intelligence environment in SA. The chapter will also examine the historical trends in SA which influence the intelligence processes and IRMF. This chapter will furthermore contextualise the current state of affairs in security and intelligence from an IRMF perspective.

Chapter Five: The Application of an IRMF for SA: Chapter Five operationalises an IRMF in SA. This chapter will develop IRMF categories that apply to SA and will further critically assess the SA environment and motivate the way forward for implementation.

Chapter Six: Evaluation, Recommendations, and Conclusion: The final chapter will report on the findings of this research. It will examine whether the research objectives have been reached and if the research questions were sufficiently answered. This chapter will also address future research and make recommendations about using an IMRF to enhance intelligence reporting in the SA context.

CHAPTER 2: INTELLIGENCE RISK MANAGEMENT A STUDY FIELD – META-THEORETICAL PERSPECTIVE AND POINT OF DEPARTURE

Risk looms large in present-day society. This is most apparent in technical catastrophes (e.g. Chornobyl), environmental changes (e.g. climate change), international terrorism and epidemics (BSE, bird flu), but it is in everyday life as well. (Zinn, 2008:1)

2.1 Introduction

Intelligence and the use of RM principles are viewed as one of the oldest professions in the world. The first use of intelligence and RM principles was cited in the Tigris-Euphrates valley about 3200 B.C., where a group called the Asipu lived (also āšipu or mašmašu). This tribe served as advisors or selected consultants to the people of the area. They advised on risky, challenging, and problematic aspects of their lives (such as marriage, risky ventures, deals in business and property). This wise group collected data and analysed the situation and gave advice on their findings. Their findings were generally based on signs from the gods, which the priest-like Asipu were incredibly qualified to interpret (Covello & Mumpower, 1985). Thus, there is reasonable certainty that business transactions have always taken place with some risk intelligence analysis. However, these two sciences (Intelligence & RM) are still in their adolescent stage regarding theoretical development, with debate on definitions ongoing. However, Tilman (2013:1) made the statement from a financial perspective: *Risk intelligence is the 'new normal' in finance, it influences a desire for leadership, ideas, and action that has emerged in response to the unsatisfactory 'new normal'. Increasingly, leadership teams are determined to spend productive energy on long-term solutions. Financial institutions and investors must develop a new competence – risk intelligence to chart a bold vision and new value proposition. The organisational ability to think holistically about risk and uncertainty, speak a common language, and effectively use forward-looking tools in making better decisions. Risk intelligence has become a key determinant of survival, success, and relevance. It equips boards and executives with new ways of seeing. Viable business models, better decisions, effective communication, and rigorous governance follow, as a result, helping financial firms to contribute to what societies need the most: sustainable economic performance, new measures of success, economic dynamism that drives growth, inclusion, and real prosperity.*

Most studies on risk intelligence and RM begin by explaining and defining what risk, uncertainty, threat, vulnerabilities, and opportunity mean because people may understand these concepts differently. Zinn (2008:2) emphasises that *a discourse into social risk behaviour is as much a discourse on defining a problem, about different values and lifestyles, power relations, and emotions as it is about 'real' risks and their rational management. However, interpreting issues in terms of risk seems to be a particular*

way of viewing our world in terms of politics, science, or everyday life. Therefore, we have to examine not just how risk is understood and discussed in society, but how we observe risk as social scientists. Therefore, through explorative methods and analysis, this dissertation will indicate what these phenomena and their inter-relation mean in IRM studies. Furthermore, this chapter will explain and define these concepts and align them with clarifying the understanding of IRM as a field of study. It will, in addition, define the influence of the developments of thousands of years of uncertainty, and analyse the theories and principles influencing modern intelligence and RM and its practices to ensure a better understanding of IRM and its influences on different fields of Social Science.

Lastly, the chapter will investigate and analyse the field of IRM to address its assessments' concepts, theory, terminology, standards, limitations, and credibility. These aspects will clarify the impact of intelligence and RM on enhancing its relevance to national security.

2.2 Etymological Basis of Intelligence, Risk, Security, Probability, Threat and Uncertainty

The study aims to ensure a good understanding of the IRM field and that this specific understanding of the language/vocabulary (etymology) is set in everybody's minds/understanding of IRM. Bracken (2008:31) argues that *Often there is not even a vocabulary or set of distinctions to facilitate discussion and analysis of the organisation's approach to dealing with uncertainty*. Therefore, the following vocabulary, as described in the sub-sections below, is of great importance to ensure the implementation of a well-designed framework that gives clarity and understanding of the IRM field.

2.2.1 Intelligence

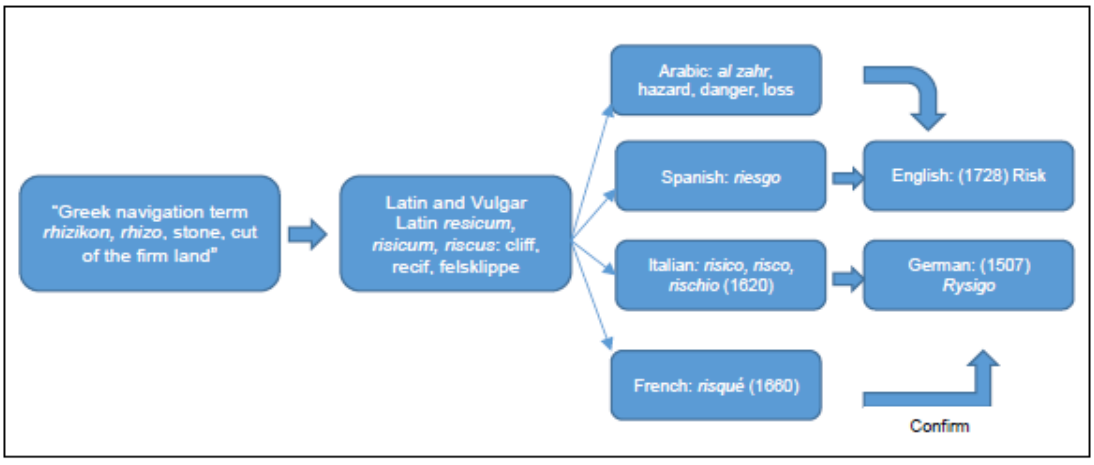
The online Etymology Dictionary (2021: index I) defines intelligence with some specific emphasis added as follows: (n.) late 14c., *the highest faculty of the mind, capacity for comprehending general truths;* **this indicates the necessity to obtain higher and specific knowledge of information.** C 1400, *faculty of understanding, comprehension,* from Old French intelligence (12c.) and directly from Latin *intelligentia, understanding, knowledge, power of discerning; art, skill, taste*, **this indicates that you obtain specific knowledge through special artistic skills (specialised training or skills must be obtained)** from *intelligentem* (*nominative intelligens*) *discerning, appreciative*, present participle of intelligere *to understand, comprehend, come to know,* **these aspects require the user to use specific lateral, critical and thinking abilities to understand (knowledge) and to analyse (comprehend) the information at hand**. The Dictionary gives a further explanation by breaking up the word intelligence *from assimilated form of inter 'between' (see inter-) + legere choose, pick out, read,* from PIE root *leg- (1) *to collect, gather*, with derivatives meaning *to speak (to 'pick out words').* **These explanations point to the activities/functions or application of intelligence processes of collection/gathering and the analysis product which needs to be compiled/disseminated (present/speak or document**

form/read) of intelligence. The Oxford Dictionary (1984) and Concise Oxford Dictionary (1999) confirm this understanding of intelligence by stating: *the faculty of understandings, the intellect* and *the ability to acquire and apply knowledge and skills*. Therefore, this study defines the word intelligence from a modern-day perspective:

> The knowledge and information obtained through specific artistic skills to make informed decisions about specific situations in state and governance.

2.2.2 Risk

Skjong (2005) describes the etymology of 'risk' by using the classical Greek origin, a nautical expression which was a metaphor for *Difficulty to Avoid in the Sea.* The term risk may be traced back to classical Greek *ριζα,* meaning root, later used in Latin for 'cliff'. Dictionaries confirm that the Latin word comes from a Greek navigation term *rhizikon, rhiza* which meant *root, stone, cut off the firm land*. From the 16th century on, the term also regarded benefit, for example, in middle-high-German *Rysigo* (used in 1507) a technical term for business, meaning *to dare, to undertake, enterprise and hope for economic success* (Skjong, 2005). Furthermore, the English verb 'risk' was used from the 1660s; the words '*risk taker'* from 1892; *risk factor* was used from 1906; *risk aversion* is recorded from 1942 and *RM* from 1963 (Oxford English Dictionary, 1989). The above explanation could be delineated as follows:



Source: Researcher's construct

Figure 2: Risk etymological development

The word *hazard,* another term integral to RM discussions, comes from a game of chance invented at a castle named Hasart in Palestine while under siege. The Shorter Oxford English Dictionary (OED, 2013) dates the word's origin in English to 1661 and defines it as 'hazard, danger; exposure to mischance or peril'. Hazard has its origins in the Arabic *al zahr*, meaning dice. The modern concept of risk only arose about 300 years ago. The OED notes that by 1719, the word denoted the *chance or hazard of commercial loss, specifically in the case of insured property or goods*. Its synonym, chance, derives from

the late Latin cadentia (from *cadere*, to fall) – *that which falls out, especially that which falls out favourably, as used in dice-playing*. The indication of the word risk is challenging to determine, and a particular root or development of the word and the use of it, as seen above, cannot be clarified with certainty.

This dissertation follows the root form as described in the OED which defines '**risk'** as the specific aspects of **danger, loss, hazard, harm and changes**. Furthermore, this dissertation will define '**hazard'** as negative event(s) created by change (potential source of harm) which endanger the organisation, institution or individual situation or objectives. ISO/IEC (International Organisation for Standardisation/International Electro-Technical Commission) Guide 73/2009 code descript hazard as a source of **risk.**

2.2.3 Threat

The threat must not be seen as an equal to describe risk; they are different. According to Damodara (2007:4), *contrast is drawn between risk and a threat. A threat is a low-probability event with substantial negative consequences, where analysts may not assess the probability. On the other hand, a risk is defined as a higher probability event, where there is enough information to make assessments of both the probability and the consequences.*

Threat has its origin as described in the OED from the old English *threat* 'oppression', of Germanic origin, related to Dutch *verdrieten* 'grieve' and German *verdriessen* 'irritate'. As an English noun, threat means a statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not done. It can also mean a threatening remark, warning, ultimatum, intimidating remark or more *rare* combination. Threat as a synonym can mean menaces, menacing, and a person or thing likely to cause damage or danger. This can be something or a person's actions that cause the possibility of trouble, danger, or ruin.

This dissertation defines '**threat'** as described in the Oxford Advanced Learner's Dictionary (OALD) (2010) as a statement in which somebody tells somebody else that they will harm them, especially if they do not do what they want. Threat is also something that possibility creates trouble, danger or disaster. This something can be a person or thing that is likely to cause trouble, danger or harm.

2.2.4 Opportunity

Opportunity is defined by the Concise Etymology Dictionary and Skeat (1980) from the French '*opportun*', and the Latin '*opportiinus',* meaning convenient, seasonable, lit near the harbour,' or 'ease of access'. In addition, the Latin *op- (ob)*, refers to near; *portus,* access/harbour.

This research defines the understanding of **opportunity** in modern RM as undertaking a risky chance to gain an advantage in a specific situation, which can go wrong.

2.2.5 Likelihood

Likelihood is defined in the OALD as the *chance of something happening*. This dissertation uses the word 'likelihood' to refer to the chance of something happening, whether defined, measured, or determined objectively or subjectively and described using general terms or mathematically (such as a **probability** or a **frequency** over a given period). The English term 'likelihood' does not have a direct equivalent in some languages, instead, the equivalent of the term '**probability'** is often used. However, in English, '**probability'** is often narrowly interpreted as a mathematical term.

This dissertation uses 'likelihood', with the intent that it should have the same broad interpretation as the term '**probability'** has in many languages other than English.

2.2.6 Probability

Probability is defined in the online Etymology Dictionary as the ancient Greek word *(eikos),* which means plausible or probable and had the same sense as the modem concept of probability - *to be expected with some degree of certainty*. Socrates also defines probability as *likeness to truth*. Bernstein (1998:48) claims *{Liber de Ludo AIeae, appears to have been the first serious effort to develop the statistical principles of probability*. However, the word itself does not appear in the book. Cardano's title and most of their text refer to 'chances.' The Latin root of probability is a combination of *probare,* which means to test, to prove or to approve, and *ilis,* which means able to be; it was in this sense of provable or worthy of approval that Cardano might have known the word. The tie between probability and randomness – which is what games of chance are about – did not come into common usage for about a hundred years after Liber de *Ludo Afeae* was published. According to Hacking, the Latin root of probability suggests something like *worthy of approbation*.

This dissertation uses ***probability*** to mean something to be expected with some degree of certainty but which can change/worthy of approbation.

2.2.7 Event

Event can be described as an occurrence or change of a particular set of circumstances, the nature of which, likelihood or consequence of an event, cannot be fully knowable. An event can be one or more occurrences and can have several causes. The **likelihood** associated with the event can be determined. An event can consist of a non-occurrence of one or more circumstances. An event with a consequence is sometimes referred to as an *incident*. An event where no loss occurs may also be referred to as a *near-miss*, *near hit*, *close call*, or *dangerous occurrence*. (ISO: Guide 73 - 2009:6)

2.2.8 Risk management

RM refers to a 'coordinated' set of activities and methods used to direct an organisation and control the many risks that can affect its ability to 'achieve objectives'. According to the introduction to ISO 31000 (2009:2), *the term RM also refers to the architecture that is used to manage risk. This architecture includes RM principles, an RM framework, and an RM process*.

2.2.9 Risk management framework

According to ISO 31000 (2009:2), an RM framework *is a set of components that support and sustain RM throughout an organisation. There are two types of components: foundations and organisational arrangements. Foundations include the organisation's RM policy, objectives, mandate, and commitment. In addition, organisational arrangements include the plans, relationships, accountabilities, resources, processes and activities you use to manage your organisation's risk.*

2.2.10 Uncertainty (or lack of certainty)

According to ISO 31000 (2009:2), uncertainty *is a state or condition that involves a deficiency of information and leads to inadequate or incomplete knowledge or understanding. In the context of RM, uncertainty exists whenever the knowledge or understanding of an event, consequence, or likelihood is inadequate or incomplete.*

2.3 Understanding Risk vs Uncertainty as Concepts

With the development of the concept of risk and RM in the 19th century, risk took up different understandings through the development of science and the understanding of these sciences regarding risk, uncertainty, and probability. *The revolutionary idea that defines the boundary between modern times and the past is the mastery of risk: the notion that the future is more than the whim of the gods and that man and women are not passive before nature* (Bernstein, 1998:1).

Uncertainty must be taken in a sense radically distinct from the familiar notion of 'risk', from which it has never been properly separated. The essential fact is that 'risk' means in some cases a quantity susceptible to measurement, while at other times, it is something distinctly not of this character, and there are far-reaching and crucial differences in the bearings of the phenomena depending on which of the two is present and operating. It will appear that a measurable uncertainty, or 'risk' proper, as we shall use the term, is so far different from an un-measurable one that it is not in effect an uncertainty at all. *It is a world of change in which we live and a world of uncertainty. We live only by knowing something*

about the future; while the problems of life, or conduct at least, arise from the fact that we know so little (Knight, 1921:199).

In the jargon of RM, risk relates to the uncertainty associated with possible future outcomes. The proverbial person in the street feels uncomfortable when facing risk because they sense a threat. For the economist, risk equates to a variety of mathematical outcomes. On the other hand, for a businessperson, it represents a potential financial loss or loss of reputation.

This separates 'risk' from 'uncertainty', where the probability of future events is not measured. Of course, the current uncertainties (for example, long-range weather forecasts) may someday become risks as science and technology progress. Therefore, understanding risk and uncertainty depend on what and where we as humans find ourselves in this uncertain world. This means our understanding/views on risk and uncertainty may differ because they will depend on what type of knowledge we have or how we experience risk and uncertainty. However, the two phenomena cannot be viewed separately as they are inter-related.

2.4 The Call for Change in Intelligence, Risk Management and National Security

Humans have lived for centuries with risks and have rethought their position on these concepts and planned accordingly to overcome them. A relevant example is the ancient Chinese farmers, who lost their crops when they transported them all by riverboat to the market via flooded rivers. After a rethink of their predicament, they developed a clever solution to divide their crops and load these smaller quantities onto their neighbour's boats. This ensured that the most significant portion of crops would reach the market. This principle of spreading risk or using RM clearly shows that humans can manage risk by mitigating its impact.

Keynes (1937) argues that *the idea of the future being different from the present is so repugnant to our conventional modes of thought and behaviour that we, most of us, offer a great resistance to acting on it in practice*. The world is changing every day due to technological developments and new designs. Humans developed new ways of doing things through research and high technological design but these developments create the riskier world that we are living in. Decision-makers are now faced with new challenges to govern their environments and make sense of all the information they have access to. New techniques and processes can assist governments' critical institutions that provide evaluated information.

Intelligence should keep up with the changing dangerous world. Lahneman (2007:2) argues that there are three different schools of thought regarding the changes that need to take place in intelligence agencies/services. According to Lahneman (2007:2), ***one group*** *believes that significant reform is not*

necessary, asserting that current efforts to significantly change how the IC does business amount to bad public policy that will ultimately cause more harm than good. Some members of this school of thought base this conclusion by arguing that since eliminating surprise attacks is impossible, the occurrence of a successful surprise attack now and then does not mean that the IC is broken. Other group members believe that some reforms are probably necessary but since no one knows what shape those reforms should take, doing nothing to prevent inadvertent damage to institutions and processes is best. The ***second group*** *believes that the IC must undergo radical change because a 'revolution in intelligence affairs' is either imminent or already in progress. (Lahneman 2007:2) This group asserts that change is not only required but also must be transformational. The* ***third group*** *of experts - the majority - adopts a position midway between these two extremes. Proponents of this view believe that significant intelligence reform is required and that determines the direction of reform efforts.*

This dissertation agrees with the third group's approach to change. An intelligence agency that cannot keep up with the changing world and environment will constantly fail its government and clients. They will not provide the necessary early warning and intelligence assessments - which is their primary responsibility and function. These services/agencies need to adapt to their environments and specifically focus their approaches to enhance their technology and intelligence tradecraft methods to enhance their intelligence processes, high-quality governance, good management, and communication.

2.5 Did an Evolution Start Taking Place in Intelligence and Risk Management?

The international incidences of terrorism, economic markets collapsing, and health threats in Africa inspired academics, journalists, scholars, and practitioners to do an introspection on the processes of intelligence and RM, as well as how these phenomena will influence the field of IRM. It is known that between the 1990 and 2000s, military affairs went through significant changes because of new practices in how forces are structured and how they apply force. Some academics believe that intelligence structures also went through these changes because of the influence of international politics, information technologies, and socio-political contexts, which influence the field of intelligence studies accordingly. In the 2000s, 9/11 and the war in Iraq forced the USA's government to change processes and coordinate measures which influenced the application of intelligence and how it was applied. From an SA perspective, several commissions, committees, and review structures were requested to review the IC's functions, processes, and objectives from 1994 to 2020. Therefore, an evolution in IRM took place during the last 15 years in different agencies in the world because of the documented and known failures through these different commissions, committees, and review panel reports.

Robertson's arguments regarding intelligence (see Herman, 1996:118) refer to the following: *threats, states, secrecy, collection, analysis, and purpose – (but) the most important of these are threats since without threats there would be no need for intelligence services.* As pointed out by Robertson, these

aspects show that change in this risk-infected world we live in will force intelligence agencies to change the way they work and how they define intelligence. In addition, Godson (1988:10) states **the mission of intelligence** as *…prognosis, the provision of warnings and estimates of future events*. This said, clearly intelligence agencies need to provide analyses, assessments and prognoses of future events/threat events, which can only be done if they stay up to date with the changing world.

Global change has already begun to take place in the intelligence world. However, how would agencies keep up with this change through mission, purpose and functional changes? This question was asked by several committees, commissions and review panels in the past 20 years to determine why intelligence failures took place and what needed to change to correct these aspects. Unfortunately, these groups did not confirm the nature, mission, and objectives for/of intelligence properly before drafting their recommendations, thus indicating their fear of radical change. To emphasise the understanding of the nature of intelligence, Troy (2008:449) makes the following four points: *Firstly, while much is made of the need for intelligence to be objective, it must be remembered that intelligence per se is* ***subjective*** *or becomes biased for a variety of reasons. Secondly, intelligence is* ***always about someone else****. Thirdly, someone else is always a* ***rival or an enemy****, or a potential rival or enemy. Fourthly, due to the nature of human nature, intelligence itself has a secure future; intelligence is* ***an instrument of conflict****, and conflict per se is, based on history and philosophy, ineradicable from this world.*

Therefore, the **mission of intelligence** has, as part of its evolution, changed from *discovering the secrets of the enemy* to *avoiding surprise attacks* (Lowenthal, 2009:2-4). Intelligence agencies' mission and their *raison d'etre* are strongly associated. Thus, Lowenthal (2009:2-4) has developed four main reasons why intelligence agencies exist in the modern era, which simultaneously provide their purpose:

- **To avoid strategic surprise:** The foremost goal of any IC must be to keep track of threats, forces, events, and developments that can threaten the nation's existence.
- **To provide long-term expertise:** This is all about continuity of expertise because all senior policy-makers are compared with the permanent bureaucratic staff (transients). They cannot be well-versed in all the matters and issues they will be dealing with. They will have to call on others who have the necessary expertise.
- **To support the policy process:** Policy-makers have a constant need for tailored and timely intelligence that will give them the background, context, information, warning, and assessment of risks, benefits, and likely outcomes.
- **To maintain the secrecy of information, needs, and methods:** The pursuit of secrecy and secret information is the mainstay of intelligence, as it makes intelligence unique. This aspect includes the counterintelligence function of intelligence.

Likewise, and as supported by this study, Handel (1989) summarises this approach to intelligence as: *In the end, intelligence is a means of comprehending reality – be it the present or future reality. Intelligence is a means – one of several instruments of power – to assist decision-makers to control their environment, to face risks, to deal with ambiguity, contradiction, evidence, and uncertainty.* Therefore, these arguments regarding the changing phenomena need to be investigated. These changes are further explored in the next section.

2.6 The Changing Intelligence Phenomena

This section will investigate the changing intelligence phenomenon from a IRM field of study.

2.6.1 Background

The change in the world due to known incidences of natural disasters and violence attract public scrutiny of intelligence and other processes like RM. Academics, scholars, and practitioners, therefore, start questioning these processes from an academic perspective. The well-known academic Gill (2009:208) (in Gill, ed al. 2009) argues that the importance of intelligence currently is not just that there is more to study but also because its performance is central to the possibility of maintaining security and safety by democratic means. This demands that Social Science examines it more systematically than in the past.

It shows similarities between what intelligence scholars and some practitioners do. They are all committed to better understanding intelligence and its processes to enhance success in these situations. Most academics, scholars, and practitioners argue regarding the theories of intelligence and theories for intelligence and if there are different roles for academics and practitioners. Johnson (International relations theorist) (in Treverton, ed al. 2009: 51-52) similarly argues that practitioners *deploy multifarious theories about their specific interests and operations. Some will be highly technical in respect of, for example, detecting evidence of radiological and chemical devices; some behavioural, for example, profiling and some sociological, such as studying motivations and dynamics of groups using violence.*

Johnson (2009:51-52) further states that academics and scholars, *on the other hand, our theories of how intelligence 'works' will be drawn from a range of psychological, economic, anthropological, organisational, political science and social theories*. This shows that intelligence as science is formed through many different theoretical borrowings to ensure that the best practices in other Social Sciences enhance intelligence processes. This dissertation proposes a new field of study in IRM to enhance intelligence studies. The interpolation of intelligence and RM can enhance the end product of the IC to give better and more informative products which the policy/decision-makers or clients can use to make properly informed decisions. Walsh (2011:xiv) argues that *the complexity of the security environment and the increasing need for different practice contexts to work in more fused ways suggest that no*

practice area holds the monopoly on good ideas; and so a more holistic and inter-disciplinary understanding of intelligence practice will benefit all academics, scholars, and practitioners.

Furthermore, Johnson (2009:52), (international relations theorist) argues that theories to understand the complexity of intelligence theories should, *after all, take us longer to unravel because human beings are much more complicated than atoms. We must bring to bear the findings and methodologies of such disciplines as history, psychology, economics, public administration (notably organisational theory), anthropology, and political science. Furthermore, the experiences of practitioners in the field will continue to be of great value, as will normative theorising.*

Where should one start to define intelligence and understand the complex intelligence environment? With the above said, how this phenomenon should be defined and understood need further analysis to ensure a shared understanding and vocabulary of the intelligence processes.

2.6.2 Defining and understanding the changing intelligence phenomena

To this extent, Warner (in Gill, ed al. 2009:17) states that the *arguments over the definition of intelligence resemble perhaps nothing so much as a trademark dispute. Each camp admits that 'intelligence' commonly signifies private information or knowledge while also serving as a synonym for espionage*. Research showed that Warner's debate regarding these views reached a point where academics, scholars, and practitioners now agree that the time has come to transcend the debate.

The problem then becomes initiating this transcendence. Intelligence still does not have a clearly defined definition. Lowenthal (2009:1) notes *Virtually every book written about intelligence begins with a discussion of what 'intelligence' means, or at least how the author intends to use the term. This editorial fact tells us much about the field of intelligence*. The father of intelligence theories, Sherman Kent (1953:ix), effuses that intelligence is made up of *three separate and distinct things that intelligence devotees usually mean when they use the word. I consider intelligence a kind of knowledge, and intelligence is the type of organisation that produces the knowledge (this part deals with organisational and administrative problems of central and departmental intelligence) …Intelligence as the activity pursued by the intelligence organisation (the intelligence [work] behind that planning must have been intense.*

Most modern-era academics, scholars, and practitioners agree that Kent has accurately described intelligence and what the basic concepts of the phenomenon (intelligence) are. Likewise, Classen (2005) argues that Kent's definition of intelligence is even more helpful as most other definitions of intelligence usually relate to Kent's definition from which they expand or motivate their views and findings. Therefore, Kent (1953) defines intelligence in three specific contexts; a kind of knowledge, a type of organisation,

and the activity pursued by the organisation. In summation, the aforementioned understanding of intelligence can be defined as advising policy-makers on how to mitigate or handle this uncertain world.

To better understand Kent's definition of intelligence, it must be analysed and expanded upon. To this extent, Warner (2006) and Bay (2007) (behaviouralism and traditionalism theorists) have analysed several authors' who expanded and gave more clarity on Kent's definition, as can be seen in the table below.

Table 2: Definitions and understanding of the changing intelligence phenomenon

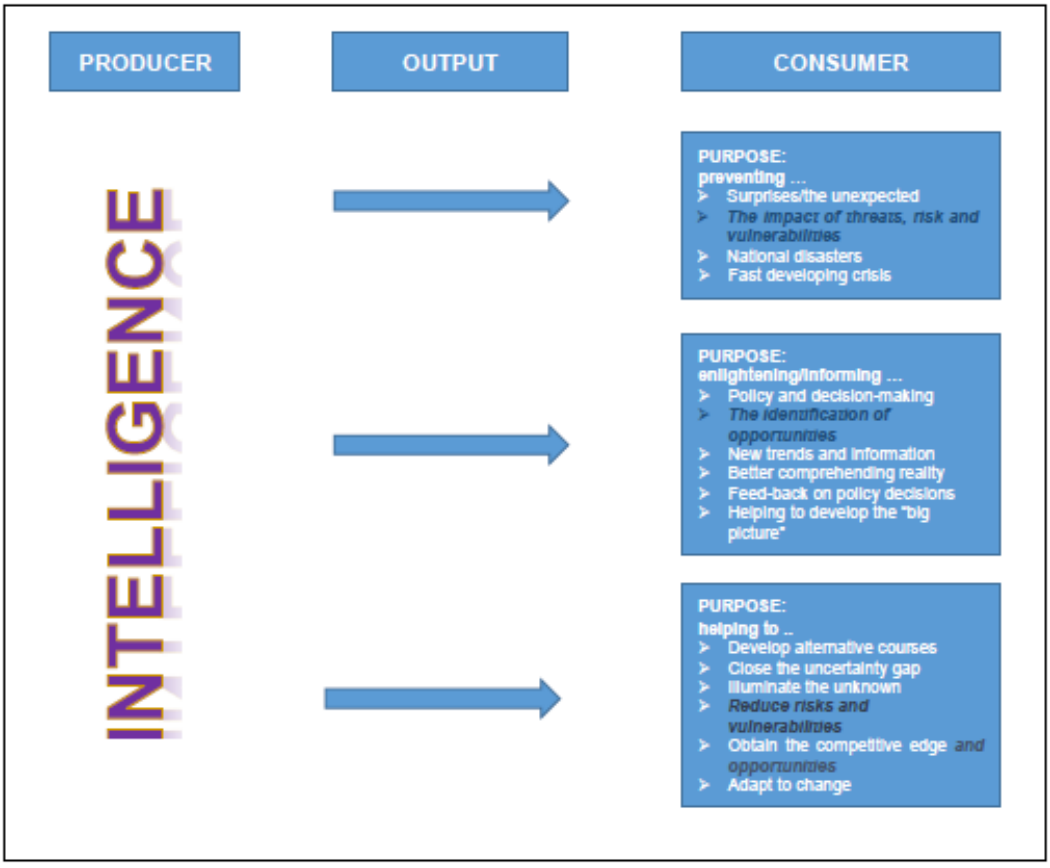
Academics	Schools of Thought	Understanding of Intelligence
Wheaton & Beerbower (2006:329-330)	Behaviouralism	Intelligence is more than information. It is a system/process.
Lowenthal (2009:66)	Classical Realism	Multi-layer intelligence process.
Sims (2009:161)	Neorealism	International relations theory – intelligence is not only defined by secrecy and covert action, it is a process by which competitors improve their decision-making.
Warner (2009:17-18)	Behaviouralism	Intelligence will impact uncertain and dangerous environments. Furthermore, the process of intelligence delivers a specific product to enhance governance, ensuring national security enhancements.
Scott & Jackson (2004:1-19)	Classical realism	Concerns with how knowledge is accepted, generated and used. Secrecy is an organising theme.
Gill & Phythian (2012:18)	Critical realism	Authors argued that any definition of intelligence should refer to specific factors. These factors can be listed as follows: • *it is more than merely information collection;* • *it covers a range of linked activities;* • *intelligence is security-based;* • *it aims to provide a warning;* • *the requirement for it arises out of a competitive environment,* • *so the gains being sought are relative ones;* • *it encompasses the potential for intelligence-led actions* • *as a consequence of its analysis, including covert actions;* • *secrecy is essential to the comparative advantage being aimed for*.
Foucault (1991)	Realism	Concepts of surveillance (governmentality) and the use of them in intelligence processes.
Clark (2002:13)	Neo/Structural Realism or Risk & Uncertainty – Behaviouralism	*Intelligence is a process to reduce levels of uncertainty. Intelligence, then, is a process, focused externally and using information from all available sources, which is designed to reduce the level of uncertainty for a decision-maker.*
Agrell (2002:1)	Structural/Functional Behaviouralism	*When everything is intelligence – nothing is intelligence*

Researcher's construct (2020)

Gill (2012:206) emphasises that *students of 'intelligence' and 'risk' have always occupied similar territories but did not normally acknowledge the fact, partly because they tended to use different vocabularies to describe their fields of interest – the former concentrated on security 'threats and the latter on safety 'risks*'. In an IRM, these concepts will inter-relate through multiple interactions (management, communication, techniques, tools and methods) which will enhance the analytical product of the intelligence structure/process. According to Buzan, Wæver and de Wilde (1998), these concepts inter-relate due to changes over the past 20 years in these fields, the change in the threat environment globally, the evolution of asymmetrical threats, and the change in the concept of security

(national/broader array of human concerns). In addition, Gill and Phythian (2018:8) argue that *the future is unknowable because it has yet to occur. Therefore, uncertainty about the shape of the future and the threats and opportunities it will bring is inevitable. Intelligence faces formidable challenges in attempting to break down uncertainty and deliver meaning and understanding on time. Perhaps, given this, the most appropriate theoretical approach to intelligence is one that explains it with ideas of risk and uncertainty. Suitably forewarned of the complexities that confront us in this area, we shall turn our attention to the theoretical landscape and consider the intelligence process more conceptually within the broader context of Social Science.*

However, Classen (2005:83) provides the figure below as an explanation of the primary functions and understanding of intelligence from the above landscape. The figure is also supported by this study.



Source: Adapted from Classen (2005:83)

Figure 3: Primary functions of intelligence

2.6.3 A meta-theory

Ritzer (2001:17-18) describes meta-theory in the same manner as Bay (2007:19), namely as the theories behind the definitions, purposes, and processes of the phenomenon to clarify the distinction. Bay (2007) and Ritzer (2001) based their arguments on the understanding that meta-theory traditionally deals with ontology, epistemology, and axiology (basing their views on Lundquist, 1993:67). Bay

(2007:5) used *meta-theory in this case to describe the theories behind the definitions of intelligence*. Ritzer (2001:18) argues that there are three types of meta-theory which are used by researchers, all generally defined by differences in their product:

- *Meta-theorising as a means of attaining a deeper understanding of theory*
- *Meta-theorising as a prelude to theory development*
- *Meta-theorising as a source of overarching theoretical perspectives.*

The above considered, more clarity is given by Gill and Phythian (2018:47), who quote Der Derian's (1992: 27) views; *What is needed in intelligence studies is a meta-theory that would take into account the fact that 'ambiguous discourse, not objective truth, is the fluctuating currency of intelligence'. The indeterminacy of what is seen or heard, aggravated by encoding, decoding, and, possibly, deception, plus the gulf between what is said and what is meant, requires an approach rooted more in rhetoric than reason. This approach – inter-textualism – 'aptly covers the field of intelligence, where there is no final arbiter of truth, meaning is derived from an inter-relationship of texts and power is implicated by the contingent nature and ambiguity of language and other signifying practices.*

Further, Der Derian (1992:46) clarifies their views by arguing that *the texts to be analysed are not just the factive ones of national security studies, but also the fictive literature of international intrigue that 'produce meaning and legitimate particular forms of power in their relation to each other*. Thus, IRM needs to be approached from a meta-theory approach as described above by Bay (2007), Der Derian (1992), Gill (2018), Phythian (2018), and Ritzer (2001).

IRM will broadly be described based on presumptions about the world. These presumptions will be based on understanding the phenomena of intelligence, RM, and national security. These phenomena will all be applied in the changing intelligence environment, as discussed above. These presumptions are fundamental to understanding why intelligence, RM, and national security are defined and why some definitions in these three fields prevail. It shows that these phenomena can inter-relate and describe why we have them, why we need them and how we should use them in one sub-study field of IRM. These concepts are of great importance to the study field of intelligence in this changing world.

2.7 Approaching Risk Management from a Theoretical Perspective

RM needs to be studied from different theorical perspective to have a better understanding and knowledge regarding it and how it will inter-relate to intelligence.

2.7.1 Background

Arad (2008:43-49) describes the inter-relation between intelligence and RM from a surprise attack perspective. The author argues that some of the recorded intelligence failures in history clearly show that something in the intelligence processes 'went wrong' and could be prevented if RM principles were applied. Furthermore, Arad (2008) argues that intelligence uses some of the 'risk assessment and management fundamentals' in the tactical, operational environment. The author also indicates that intelligence practices already specifically use *probabilistic measurements, evaluation of risk and the use of scenarios, there is a wide use of explicit risk-control and management tools, such as backup systems, and risk reduction via diversification and redundancy.* This motivates the use of RM inter-related with intelligence. This should not create a problem in the intelligence processes because their practitioners and management are trained in 'probability thinking' used in early warning applications. Arad (2008) argues that it could not be understood that a proper and 'comprehensive RM doctrine for intelligence' was not developed.

Through an explorative investigation into RM, it was found that ORM is the recommended application in RM to inter-relate with the sequential process of early warning specifically. Therefore, Bracken *et al.* (2008:6) also argue that *RM is about insight, not numbers. It is not the predictions that matter most but the understanding and discovery of the dynamics of the problems* (Bracken, 2008:6). Bracken further argues that *RM necessarily involves how risk is perceived, and how individuals, groups, and organisations process it. This is a very complicated and interesting subject. Different individuals assess likelihood (Probability) in different ways; they often also see the consequences of what could take place differently. No methodology will ever overcome these tendencies. Nevertheless, being able to lay them out for clear discussion, with an* ***appropriate vocabulary****, is a step toward a more productive discussion.*

The above arguments clearly show that new ways of data/information collection and management should be applied in the modern world. This means that existing methods of applying intelligence and RM need to change to ensure that the primary objective of these phenomena will encourage managers to be sensitive to other forms of data than the everyday typical numeric statistical data/information to make decisions. Blunden and Thirlwell (2010:19) state that *Quantitative analysis undoubtedly has its place, but the actuaries are applying intelligent RM* to be more objective regarding their reporting of the risk faced today. Fingar (2011:25) argues what intelligence should be and what it should not do in the fast-changing modern world. The author states that *intelligence is not supposed to—and in my experience very seldom does— advocate specific courses of action. Its primary purpose is to provide information and insight that will enhance understanding of the core issue, how it relates to other matters and the possible consequences of alternative courses of action.*

Stated differently, the primary purpose of intelligence inputs into the decision-making process is to reduce ***uncertainty***, ***identify risks*** and ***opportunities***, and, by doing so, deepen understanding so that those with policymaking responsibilities will make 'better decisions'. These aspects regarding RM should be further investigated as to how they inter-relate with intelligence.

2.7.2 The challenges to applying risk management in the intelligence environment

Arad (2008:43-49) describes the challenges in implementation that practitioners are facing regarding RM in intelligence processes, notwithstanding that some aspects of RM are used and are very well understood by intelligence practitioners and management. However, there is no doctrine on IRM written or promulgated. Arad (2008) argues that there are specific aspects and 'obstacles' regarding the types of risks (internal and environmental risks) that need different tools to assess these risks, which created a problem in the intelligence processes. The intelligence processes viewed environmental risks as threats from the external environment and failed internal processes as operational risks from the people, processes, and technology. From an intelligence process perspective, these different views are the 'main obstacle' to using RM in intelligence. Environmental risk is generally assessed in other fields as a special type of risk with a 'malicious intent'. These aspects of environmental risk (which are defined as a threat) are not in line with the nature of security risks. These aspects of environmental risks *lower the relevance of statistics and probabilistic distributions* in the RM processes. Notably, a military adversary does not *commit himself to statistics* in planning or executing an attack (Arad, 2008: 43-49).

Furthermore, Arad (2008:43-49) indicates that different tools analyse the abovementioned risks (environmental and internal operational risks). Some organisations use two different structures to handle these risks. These differences can make intelligence a hindrance. Intelligence analysts usually manage these risks from their core business attack objective and do not use different risk tools in these circumstances. Therefore, intelligence structures are not identifying and controlling these types of risks like other organisations because this *is an inherent tautology that erodes the effectiveness of RM in this context*. Arad (2008:45) furthermore states that intelligence does typically not separate these two risks, *since most tasks include operational aspects while concurrently handling environmental risks*. Arad (2008:47) uses 'deception' as an example in operational situations where an environmental risk will turn into an operational risk if not correctly identified. These actions can lead to the attacker misleading and disrupting the defender's early warning system.

In conclusion, Arad (2008:43) indicates that the sequential nature of an early warning system clearly shows that ORM suits the intelligence processes better. The author argues that *ORM underlines organisational processes, procedures, and mechanisms, which places an enormous responsibility on supporting national stability*. If intelligence agencies do not comply and implement these specific responsibilities correctly, it can lead to severe losses. Intelligence units are viewed as national RM

mechanisms that exist to cope with any attack. Due to the uncertainty of these events or incidents, RM tools can be used to analyse these aspects because being *systematic, comprehensive, and pre-emptive makes RM a 'potent instrument'*. These aspects of RM provide *a comparative overview of the entire system and the processes and interactions within it. Recent intelligence failures have shown that this wide-angle perspective is of the utmost necessity*. Therefore, ORM needs to be further analysed to determine how it will influence the intelligence environment.

2.7.3 Defining operational risk management

Stern and Wiener (2006:393) argue that *decision-makers developing counterterrorism measures need mechanisms to ensure that sensible risk analysis precedes precautionary actions*. They further emphasise that *such a mechanism currently exists to review and improve or reject proposed precautionary measures against health and environmental risks, but not, so far, for counterterrorism and national security policies* (Stern & Wiener, 2006:393). Real-world RM, if properly implemented and understood, will influence practitioners, specifically operational risk managers, to be passionate about their discipline. Operational risk exists in every industry and every endeavour. It exists in massive global 'multimedia extravaganzas' and small local events.

Blunden and Thirlwell (2010:8) indicate that the most widely used definition for ORM in the financial environment is by the Basel Committee on Banking Supervision: *The risk of loss resulting from inadequate or failed processes, people and systems or external events. The committee indicated in their publication that this definition includes legal risk but excludes strategic and reputational risk*. It does appear that the Basel ORM rules are applicable across the board of all institutions and industries. Most academics, practitioners, and managers define ORM based on the Basel definition or very close to it. The International Convergence of Capital Measurement and Capital Standards: BS 31100 (2011), enhances the definition of Basel ORM as follows: *The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events*. If this definition is broken down it shows that there is a loss because of risk(s). That said, a loss because of risk must be anticipated. In addition, a lost event can be defined as money, people, or infrastructure. The reasons for this 'loss' are indicated in the definition and can be described as i) inadequate, failed, or poor process; ii) inadequate or human errors, iii) inadequate, failed, poor integrity or suitability of the systems, and iv) external events. This link to events was illustrated by Young (2008:7) and the Britain Bankers Association Gold database, with some emphasis added for an IRM purpose in the table below.

Table 3: Causes and events/Sub-categories of operational RM

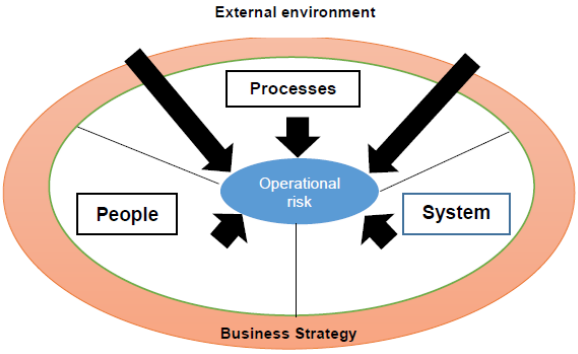
RISK FACTORS/CAUSES	EVENTS
People/Employees	• Errors • Internal fraud • Employment law • Absence/loss of key staff • Wrongfully involved with criminal activities (Terrorism, Espionage, Subversion or Sabotage)
Systems (technology)	• System failure • System integrity • Outdated systems • System suitability • System support
Process	• An unsecured or safe process that hampers service rendering; • Documentation which is not fit for purpose; • Errors in processes; • Project management failures; • Internal/external influences on the processes • Reporting
External environment/ factors or events	• External crime and specifically fraud; • Outsourcing (and insourcing) risk; • Natural and other disasters; • Regulatory risk; • Political risk; • Utilities' failures; • Competition.

Source: Adapted from Young (2008:7) and British Bankers Association Gold database

With this definition in mind and looking at the mass media reports or news, one will quickly identify the losses that people, organisations, and states suffer daily because of *failed processes, inadequate people, broken systems, and violent external events.* (Young, 2008:7) These losses are **mainly** due to operational risk events which were not adequately managed or analysed. ORM needs to be further investigated to determine how it can influence the institutional environment from an intelligence perspective.

2.7.4 Key areas of operational risk management

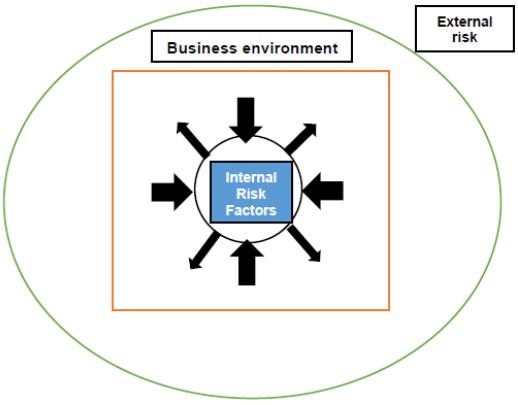
From the definitions and views mentioned above regarding ORM, there are specific key areas (namely inter-relationships, factors, and the environment in which ORM functions) that need to be clarified for a better understanding of ORM from a theoretical perspective. ORM functions in two main areas in all institutions/organisations or states. These two areas are identified as internal and external factors. Young (2008:7) argues that these internal factors *should be reviewed according to a set of three components: capacity, capability, and availability*. Furthermore, they indicate that external factors must be assessed against the external aspects which directly 'influence the business' of the organisation. As seen below, Young (2008) depicts the factors mentioned above, which can influence the organisation's internal and external business environment.



Source: Adapted from Young (2008:8)

Figure 4: Inter-relationship between the business environment, external risk factors, and internal risk factors

The factors mentioned above can also exist *within the overall framework of the organisation's business strategy* (Young, 2008:9). This environment is illustrated in Figure 5 below.



Source: Adapted from Young's (2008:9) adaptation of Rachlin (1998:117)

Figure 5: Key areas of operational risk

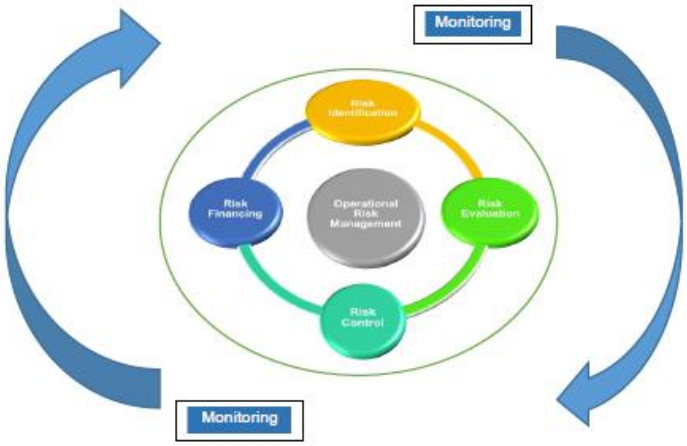
The above figures indicate that organisations need to focus their risk and uncertainty on the external and the internal environment. Tilman (2013:2) argues *that the presence of risk – and the critical importance of effective decision-making under uncertainty – permeate strategy, business models, leadership, and cultures across the financial industry. To chart a bold vision for relevance and lasting success, financial firms, and institutional investors must foster a new type of competence –* ***risk intelligence*** *– that we define as: the organisational ability to think holistically about risk and uncertainty, speak a common risk language, and effectively use forward-looking risk concepts and tools in making better decisions, alleviating threats, capitalising on opportunities, and creating lasting value.*

This risk intelligence includes all the relevant areas of an organisation that will influence and direct a strategic imperative and a decisive adaptive advantage. This provides the necessary new ways these executives or policy-makers will view the future and manage uncertainty. Kaplan and Mike (2012:11) state that *A firm's ability to weather storms depends on how seriously executives take RM when the sun is shining, and no clouds are on the horizon*.

2.7.5 The operational risk management framework and processes

RM can only be implemented if it is done through a well-designed framework and structured processes. An ORM framework should cover all aspects of the organisation's business. The organisation should focus on developing this framework and later include other aspects that are more relevant, specifically, to the strategic and external environment. These frameworks will inter-relate well and will ensure that an integrated approach to ORM is followed. During this development phase, the focus will be on an ORM strategy, ORM processes, ORM governance structures, and the environment and culture for managing ORM.

The ORM processes will primarily ensure that risk avoidance is included, risk acceptance levels are agreed upon, the risk that can be transferred is identified, risk reduction areas are identified, and safety or loss control procedures are approved and implemented. Young (2007:33), illustrates these perspectives in Figure 6.



Source: Adapted from Young (2008:33)

Figure 6: ORM processes

2.8 The Physiological Control by Intelligence Practitioners, Risk Managers, Analysts or Users

Every person will react in four different ways to the incident, depending on the person's knowledge, education, culture, and previous experiences evolved from a fear, freeze, fight, or flight response. These responses will influence the product analysis by these analysts, managers, or practitioners during RM processes. This can influence the decision-making processes of policy/decision-makers or clients who receive these IRM products. These aspects can hamper the proper governance, implementation, and security of the state (national security). These aspects will tempt the people involved to respond to these incidents with an automatic response by throwing time, money, and all resources as a quick fix. Due to these 'modules', as Heuer (1999:ix) calls them, the responses by analysts, managers, and policy-makers are understandable. The personnel involved with IRM processes on all levels (strategic,

coordination, and departmental) should be adequately trained and made aware of these analytical traps, which can influence their thinking processes and decision-making. These aspects are also informed by Kahneman (2011:366). According to psychologists Kahneman and Tversky (1973:207–232), s*omething similar can happen when we estimate probabilities. Just as the visual system relies on various heuristics to estimate size, the risk system has its bag of tricks to estimate probabilities. Moreover, just as the heuristics of the visual system sometimes led to optical illusions, the cognitive shortcuts we use to estimate probabilities can lead us to make systematic errors.*

These views clearly show that when working with uncertainty and specifically with probabilities, the analysts must be aware that their thinking can be influenced by their mindset, observations (viewing), and set biases. Analysts, managers, and practitioners must control these aspects cautiously. These aspects of the human makeup can severely influence the outcome of their product (advice) to the policy/decision-makers. However, Honig (2007:702) and Wohlstetter (1962:397) assert that intelligence failures are not the product of analysts' negligence or stupidity, but rather the result of inherent cognitive biases that affect *…honest, dedicated, and intelligent men. It emphasises that the cognitive shortcuts people employ to cope with the volume of the information they are bombarded with—much of it contradictory and ambiguous—inevitably lead to mistakes in judgment. Since these biases are inherent in human nature, they affect all intelligence analysts.*

Honig (2007) and Wohlstetter's (1962) arguments reconfirm the importance of well-recruited and trained analysts in the intelligence communities, to drive the IRM processes to ensure better and quality products that enhance national security. Further, these influences will form specific methods and tools to be used in the general practices of RM. Therefore, these changes need more investigation.

2.9 Risk Management as a Concept in General Practice

Enterprise Risk Management (ERM) is a shift from the traditional approach to RM. ERM, and specifically ORM, will be adopted and used throughout this study. These two types of RM approaches will be used interchangeably to overcome the challenges of RM use in the intelligence processes. The adoption is necessary, as described and argued by Dabari and Saidin (2014:627), as *quite recently, ERM has become the practice standard across the world because the silo or traditional approach has failed to produce the desired results and that the financial disaster continues to occur regularly*. *Despite the growing importance of RM*, Arad (2008:43-49) still argues that RM is not used in intelligence that frequently, and no doctrine for the use of it in early warning and specifically in intelligence is drafted by academics, practitioners or scholars. The ERM processes are very clearly illustrated by *ISO 31000*, as seen in Figure 7 below. However, risk is an integral part of life that has to be managed. In business life, it has been increasingly enshrined in codes of corporate governance since the early 1990s. The Cadbury Report (1992) was the first of these, leading to the UK's first *Combined Code of Corporate Governance*,

which was published in 1999, along with the Turnbull Report on internal controls. Cadbury was closely followed by the Toronto Report in Canada and King Report in SA (1994), with similar reports and recommendations in Australia and France in 1995. The OECD Principles of Corporate Governance, first published in 1999, include the paragraph: *An area of increasing importance for boards and closely related to corporate strategy is risk policy. Such policy will involve specifying the types and degrees of risk that a company is willing to accept to pursue its goals. It is thus a crucial guideline for management that must manage risks to meet the company's desired risk profile.*

Nonetheless, this study postulates that there is a relationship between RM principles, frameworks, and processes, as indicated in Figure 7 below. Notably, the above arguments will force organisations to review their strategies regarding the implementation of RM. They will have to consider how to approach RM, and several challenges will determine this implementation, namely poor knowledge of RM by members of the executive, lack of professionals, lack of risk training and education, as well as lack of a framework that supports the development of skilled and capable workers in the intelligence sector. Furthermore, the characteristics, external audit quality, internal audit effectiveness, human resources competency and regulatory influence will also affect implementation, specifically in the intelligence environment, as intelligence practitioners are very set in their ways. Limited studies or research exist on using RM in the intelligence sector. It was indicated earlier, specifically by Arad (2008), that no doctrine or policies are available on the phenomenon. Therefore, the proposed theoretical framework in this study may be a valuable tool for academics to understand these antecedents in future and improve them.

Academics, scholars, and practitioners generally question the RM environment when modern ERM views influence the practice. According to Siu (2009:1), *risk share a common generic structure in terms of which of their various characteristics can be systematically represented and understood (i.e. 'one-size fits all' theory)? Alternatively, are risk issues inherently disordered, inevitably different from each other, and open to unaccountably different interpretations and actions by different people (i.e. risk is situational, site-specific, and context-specific)?*

Siu's (2009) arguments are specifically relevant to the intelligence environment because most intelligence processes reflect risk-situational, site-specific, and content-specific characteristics due to the complexity of the environment in which they work. Likewise, it was found that these aspects apply to intelligence and most environments where practitioners apply risk analysis or assessment. Furthermore, Zinn (2009:8) argues that *there are diverse views and interpretations of risk*. In the literature, the risk is often regarded as 'analysis,' 'social constructs', 'feelings' and so forth.

Limited studies were devoted to exploring the diversification of the meanings, and there is a lack of (meta-) risk theory that explains their co-existence. Zinn's (2009) research depicts *the development of*

a meta-theory of risk to fill these intellectual gaps and identifies several essential elements of the developed theory. They provided the table below to illustrate their views regarding the diversification of risk theories.

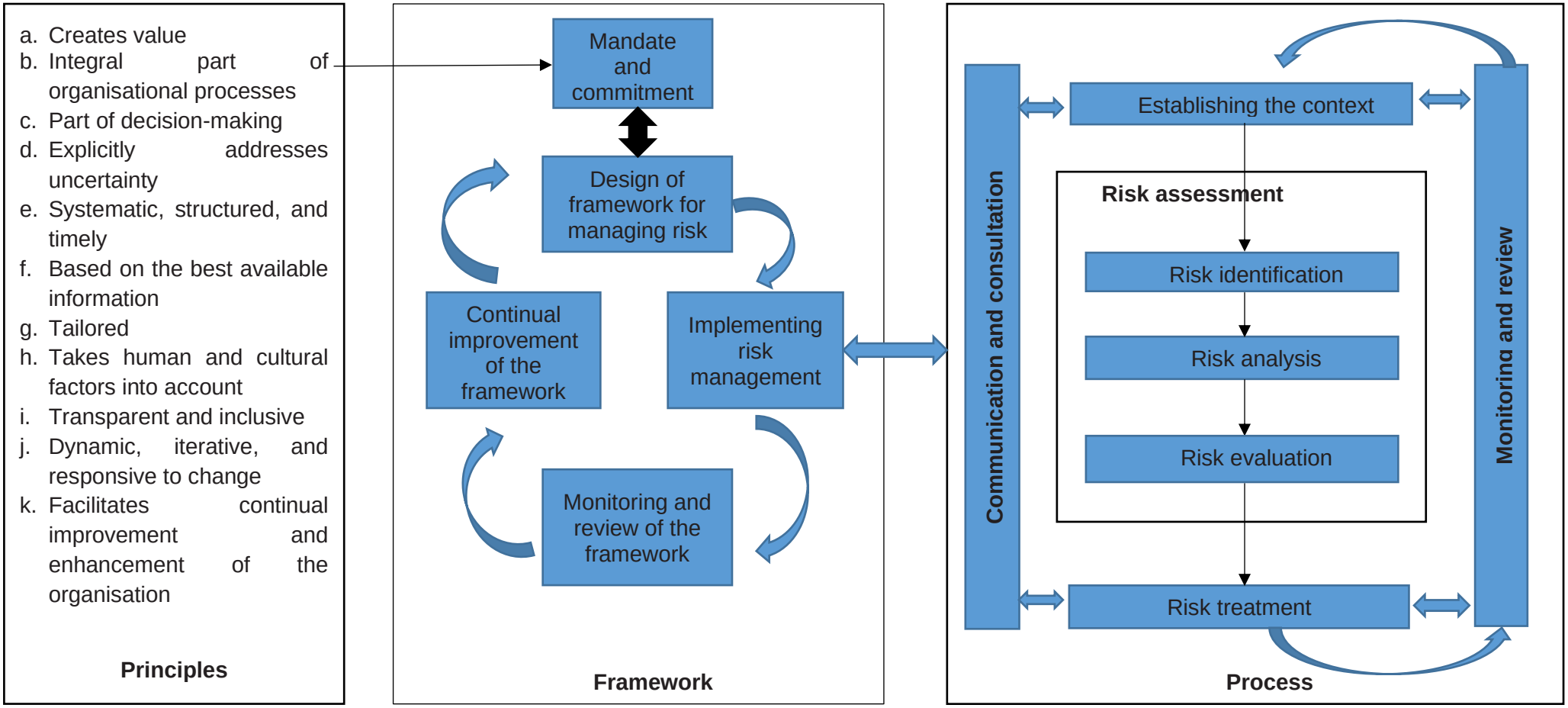
Table 4: Risk epistemology in different disciplines and approaches

Risk as ….	Perspective	Approaches
Real and objective	Objective calculation of events	Technical risk assessment, insurance, epidemiology, toxicology
Subjectively biased	Objective risks are subjectively perceived and calculated	Psychometric paradigm, rational choice: objective/subjective utility
Socially mediated	The subjective experience of real risks is socially mediated	Edgework
Real and socially constructed	Reality and talking about risks mutually influence and produce each other	Risk society
Socially transformed	Real threats are transformed into risks for sociocultural boundaries	Cultural theory
Socially constructed	Events are risks insofar as they are part of a calculative technology	Governmentality
	Risks are socially ascribed decisions	Systems theory

Source: Adapted from Zinn (2009:8)

Siu (2009) and Zinn's (2009) arguments are further expanded by ISO 31000, which acknowledges this similarity by stating: *Although the RM process is often presented as sequential, in practice it is interactive' process which will review its findings by re-look its data and findings*. In conclusion, these practices argued above are summarised by Louisot and Ketcham (2014:4) from a national security perspective: *Nations themselves have to organise their internal (police and judicial system) as well as external (national defence) security in an ever more complex and fluid environment, not to speak of their reputation in the light of the fight against corruption and money laundering. Therefore, political leaders should regularly review their approach and engage in an interactive risk assessment and management (ERM) approach.*

These arguments show that *risk is incorporated into so many different disciplines, from insurance to engineering to portfolio theory, that it should come as no surprise that it is defined in different ways by each one, which in turn influences the use of ERM in these institutions*. (Louisot and Ketcham 2014:4) As mentioned above, the figure below visually describes the relationship between RM frameworks, processes and principles based on ISO 31000 concerning ERM.



Source: Reproduced from and based on ISO 31000 (2009:vii)

Figure 7: Relationship between the RM principles, framework, and process

2.10 A Meta-theoretical Approach in National Security

Buzan (1991:432-433) made the following statement regarding the change in national security: *Security is taken to be about the pursuit of freedom from threat and the ability of states and societies to maintain their independent identity and their functional integrity against forces of change, which they see as hostile. The bottom line of security is survival, but it also reasonably includes a substantial range of concerns about the conditions of existence. Quite where this range of concerns ceases to merit the urgency of the 'security' label (which identifies threats as significant enough to warrant emergency action and exceptional measures including the use of force) and becomes part of everyday uncertainties of life is one of the difficulties of the concept.* In addition, Hough (2002:3) states that Mathur (1996) conceptualised national security as *… several factors that will determine national security in any given country, namely geographic and geostrategic conditions; human and material resources; the level of industrial and economic development; political conditions; sociocultural conditions; military power; and the types of external and internal threats.*

However, their comprehensive view of national security reflects some of the problems of over-extending the concept to include virtually all societal ills. Furthermore, Dokken (2001:2) describes that *By the end of the Cold War, there was a general perception that security was closely related to states and the sovereignty of states*. After Machiavelli (1469 – 1527), Hobbes (1588 – 1679), and Rousseau (1712 – 1778) introduced their classical works, security was referred to as *the security of states*, with the military apparatus playing the most important role in its maintenance. Security was ***traditionally*** considered to be synonymous with military security because most challenges to a state's integrity seemed to come from external violence (Dokken, 1997:69). In their research, Gill (2012:206) noted Wæver and Wilde (1989): *There remains a key distinction, but over the last 20 years, these fields have converged for several reasons including the proliferation of asymmetrical threats and broadening of the concept of security beyond the 'national' to a broader array of 'human' concerns.*

Due to the changes in the world, 'human security' starts playing a larger role than the traditional view of national security. Dokken (1997) further argues that traditional security interpretations have become outdated after the Cold War's end, as well as rapid geopolitical changes. Dokken (1997:69) identifies three significant focus areas for security by states which influence states to focus more prudently on these aspects:

(1) threats to the international community as a whole, primarily linked to terrorism;

(2) threats against the individual, against his or her physical survival, human rights, basic welfare rights, and so on; and

(3) threats to countries at a regional level.

This change of focus is central to the subject of this dissertation. It clearly shows that national security should be approached from a widening security perspective, influencing the intelligence environment. Therefore, the intelligence and RM theories approach to IRM will be more meta-theoretical.

The above changes, as discussed, are significant and specifically tailored for Africa. SA has identified these aspects and included them in its Constitution. The Constitution (RSA, 1996: s 198) upholds these views: *national security must reflect the resolve of SA, as individuals and as a nation, to live as equals, to live in peace and harmony to be free from fear and want … '(a classic expression of human security)*. Cawthra (2013:6) expand on Dokken (1997) and the Constitutional statements and show that further *variations on this formulation have been repeated in all government security-related documents, including intelligence legislation, safety, and security policy and foreign policy (where there is also an emphasis on multilateralism, peaceful resolution of disputes and African and developing-world solidarity*. Notwithstanding, these aspects are included in some African states' national security views however application lacking. Dokken (1997:69) indicates that *both causes and consequences have taken different forms in Africa as compared with Europe and the rest of the Western world*. She further argues that African states *have been among the most important 'breeding places' for terrorists, lack of development is steadily threatening peace and stability in African countries, forcing inhabitants to flee their home ground for uncertain futures in the West. Furthermore, she argues that because of these aspects materialising in Africa, more than anywhere else, African states face the daunting task to live up to these 'security challenges* (Dokken, 1997:69).

Further to this, Hough (2013) describes a widened human security framework that countries worldwide have used to change their approach to national and global security. Gill (2012) refers to Sheptyki (2009:166-172), stating *If for instance the dominating realist perspective would be exchanged for a human security paradigm such a rethink would have important consequences for the IC*. This emphasis shows that change in thinking and theory is needed regarding intelligence and its approaches to national security.

Furthermore, Hough (2013:12) explains these views through statistical data tables from different surveys, which clearly show that people think about national security from a different perspective than during the Cold War era. The following two tables give a clear picture of people's views from an international/global perspective and also from Africa's perspective.

Table 5: Single biggest fears in the world[a]

1.	Crime	27[b]
2.	Terrorism	15
3.	Health/economic insecurity	13
4.	Accidents/natural disasters	12
5.	War	8

Notes

a. Based on a survey of 6 043 people in 11 countries: Brazil, Canada, France, India, Japan, Russia, SA, Thailand, USA, UK. They were asked to name the single greatest threat to their life.
b. Some respondents did not answer.

Source: Human Security Centre (2005: 52 – 2)

Source: Reproduced from Hough (2013:12)

Table 6: Single biggest fears of Africans[a]

1.	Economic insecurity[b]	37[d]
2.	Disease[c]	21
3.	Corruption	7
4.	Illiteracy	6
5.	War	6
6.	Political conflict	5
7.	Environmental destruction	3

Notes

a. BBC World Service poll of 7 671 people from Kenya, Tanzania, Mozambique, Ghana, Nigeria, Cameroon, Malawi, Zambia, Rwanda, and Côte d'Ivoire.
b. Economic Insecurity conflated from the poll's categories of poverty (24%), unemployment (10%) and poor economic development (3%)
c. This Category collates HIV/AIDS (14%) and poor health (7%)
d. Some respondents gave no answer

Source: BBC (2004)

Source: Recreated from Hough (2013:12)

In conclusion, this dissertation will uphold the definition of national security from a human security perspective as indicated in Chapter One. It is as follows: *National security is the first and most important obligation of government. It involves not just the safety and security of the country and its citizens. It is a matter of guarding national values and interests against both internal and external dangers – threats that can potentially undermine the security of the state, society, and citizens. It must include not just freedom from undue fear of attack against their person, communities, or sources of their prosperity and sovereignty, but also the preservation of the political, economic, and social values – respect for the rule of law, democracy, human rights, a market economy, and the environment – which is central to the quality of life in a modern state* (IWGNS, 2013:3).

2.11 Conclusion

In summary, from exploring the three phenomena, it becomes evident that their inter-relationship must have a properly defined vocabulary, language, and understanding to ensure a dialogue regarding uncertainty and risks. The changes in intelligence, RM, and national security after the Cold War era tempted several states, institutions, and specific intelligence agencies to convert to risk intelligence

practices to ensure they could manage uncertainties, risks, vulnerabilities, and opportunities. All three phenomena cannot be clearly defined, or alternatively, there is no renounced theoretical approach to these phenomena that define them. Bay (2007), Gill (2012), Gill and Phythain (2018), Phythian (2012) and Warner (2009) indicate that a more meta-theoretical approach in intelligence studies needs to be followed to gain more clarity regarding this changing world. Wirtz (2017:31) reminds us of Handel's paradox, which subverts the usual risk calculation of likelihood multiplied by impact and lies at the heart of the theory of surprise. Handel (1977:468) further clarified that *the greater the risk, the less likely it seems, and the less risky it becomes. In fact, the greater the risk, the smaller it becomes*. These aspects show that intelligence agencies need to change their processes, thinking, and final products, which need to inform, advise, and direct the policy/decision-maker or client of their products. These products must inform regarding threats or potential threats, as well as which risks, vulnerabilities, and opportunities there are for these leaders. Tilman (2013:2) defined risk intelligence as: *The organisational ability to think holistically about risk and uncertainty, speak a common risk language, and effectively use forward-looking risk concepts and tools in making better decisions, alleviating threats, capitalising on opportunities, and creating lasting value*.

Furthermore, Chapter Two clarified the three phenomena's definitions, vocabulary, language, processes, and objectives. The chapter argued that there is a change needed in intelligence, RM, and national security. However, the three groups differ regarding the change that needs to occur, and this dissertation supports that modern and calculated changes are needed in the processes and the end products of intelligence agencies. These changes should include all the areas of the processes and should not only focus on one specific element. The chapter also shows that a very specific inter-relationship is needed between intelligence and RM to cover risks, vulnerabilities and opportunities. Arad (2008) indicates that intelligence agencies and management are already using aspects of RM in their intelligence processes and thinking. The author cannot understand why a doctrine is not already developed for the use of RM in the intelligence environment, as in other Social Sciences and business processes. The chapter further indicates that some institutions use different RM processes because they need to implement RM in the external and internal environments, which are not separated from the intelligence processes. These activities show that the inter-relation between intelligence and RM has some challenges that need to be clarified by agencies before they apply different tools and methods in the intelligence environment. This chapter furthermore serves as a pretence to the theoretical construction of an IRMF, as will be presented in the next chapter.

CHAPTER 3: AN INTELLIGENCE RISK MANAGEMENT FRAMEWORK

There is little other publicly available literature on what makes an effective intelligence framework in different contexts, and how researchers and practitioners can work to build better frameworks that can adapt to the changing security environment (Walsh, 2011:92).

3.1 Introduction

This study's main purpose is to conceptualise an IRMF which will provide all the necessary management tools for the intelligence service/agency to deliver a professional strategic product to the policy-maker, executive or client. To conceptualise this IRMF, the previous chapter's theories must be shaped into a framework that includes all the necessary aspects, principles and functions to ensure its proper implementation. Due to the complexity and changing of the global environment, intelligence services/agents need to make adjustments to handle these threats and risks more systematically. One of these changes regards using Social Science tools such as RM in the intelligence processes to provide a more reliable early warning, as well as strategic products. This raises the question of how an IRMF and/or assessment module(s) (according to this study) should be developed and conceptualised within an intelligence framework. To understand and define both the environments of intelligence and RM, one needs to go back to Chapter Two and understand the root theories of these concepts to clarify and describe their inter-relationship and how these concepts can support each other in a specific framework.

Chapter Three builds on the theoretical concepts of Chapter Two. This chapter will describe and construct the different theories and elements which influence and form the IRMF. In addition, this research selects and motivates a theoretical point of departure that forms the basis for developing an IRMF, which will influence and enhance intelligence analysis. Walsh (2011:91) explains the importance of intelligence frameworks: [in]…*simple terms, there has been insufficient reflection by scholars and practitioners on either the structural or functional components that make up intelligence frameworks. While components of frameworks – collection, analysis or facilitating activity such as technology – are discussed at length generally there is less discussion on how these fit together, and whether they are producing the kind of intelligence support decision-makers can use.*

Therefore, this chapter will conceptualise the inter-relation and collaboration between intelligence and RM, which were explained in Chapter Two. It will focus on how intelligence and RM fit together to enhance the intelligence products which advise the policy-maker/client on national security. Furthermore, Chapter Three conceptualises an IRMF with the benchmark standards of framework design and compliance aspects. Lastly, this chapter will also utilise a comparative analysis of relevant

case studies in the construct of an IRMF. The next section will expand on how a framework should be understood.

3.2 Understanding Frameworks

An explanation of the policymaking process rests in theories and models, which should be (but typically are not) grounded in a framework (Ostrom, 2007:25). As Ostrom (2007) argues, frameworks play a critical role in accumulating knowledge. Frameworks bind inquiry and direct the analyst's attention to critical features of the social and physical landscape. Frameworks provide a foundation for inquiry by specifying variable classes and general relationships among them. Frameworks organise inquiry but they cannot in and of themselves provide explanations for, or predictions of, behaviour and outcomes. Explanation and prediction lie in the realm of theories and models. Alternatively, as Ostrom (2007:25) states, *Frameworks organise diagnostic and prescriptive inquiry. They attempt to identify the universal elements that any theory relevant to the same kind of phenomena would need to include*. Finally, frameworks provide a meta-theoretical language that can compare theories, allowing policy scholars using different theories to use a common language, learn from one another, and identify pressing questions to pursue.

This dissertation will use frameworks described by Walsh (2011:91-95) from five countries (New Zealand, USA, UK, Canada, and Australia) to explore an IRM environment. This will furthermore direct a new design in the intelligence study field and provide a better understanding in order to apply the changes in intelligence processes to provide an enhanced product. These products will inform policy/decision-makers to manage uncertainty and risk in their environment. These goals can be achieved by an IRMF which is appropriately structured.

3.3 The Need for a Proper Structured Intelligence Risk Management Framework

Walsh (2011:93) argues that intelligence frameworks are fundamental because they clarify the core areas in the intelligence processes. The framework provides the necessary details regarding tasking and coordination mechanisms, methods of collection, analysis, and intelligence production processes, which ensure a holistic intelligence process is followed in the institution. Frameworks and properly planned structuring will ensure creativity with the workforce or people in the system. Pace (2018:67) argues that from a cyber security perspective, *threat intelligence frameworks provide structures for thinking about attacks and adversaries. They promote a broad understanding of how attackers think, their methods, and specific events in the attack lifecycle. This knowledge allows defenders to take decisive action faster and stop attackers sooner. Frameworks also help focus attention on details that*

require further investigation to ensure that threats have been fully removed and that measures are put in place to prevent future intrusions of the same kind.

Frameworks help share information within and across organisations. They provide a common grammar and syntax for describing the details of attacks and how those details relate to each other. A shared framework makes it easier to ingest threat intelligence from sources such as threat intelligence vendors, open-source forums, and Information Sharing and Analysis Centres (ISACs). These aspects, as pointed out by Walsh (2011) and Pace (2018), are also part of the IRM environment, as indicated in Chapter Two. In an IRMF, several aspects must be set to ensure proper implementation of an IRMF, namely i) common language/vocabulary; ii) good communication, planning, and understanding (through good training) by the organisation; iii) good management, and iv) liaison with public entities to obtain more clarity regarding the threats, risk, vulnerabilities, and opportunities the country is faced with.

This study postulates that an IRMF will ensure that there is better structuring in the IC. These structures will ensure that each of the different levels in the framework function correctly and that the people who work in that specific level apply the correct aspects to ensure they achieve their objectives. In an IRMF, there are three different enhancement levels with specific responsibilities allocated to each level:

- The **executive governance level** is responsible for policy formulation and decision-making regarding uncertainties and risks;
- The **coordinating level** needs to coordinate all IRM products from the different intelligence departments to ensure holistic inputs can be accomplished; and
- The **departmental level** is the IC and other government departments that are of interest to advisors and national security importance at the given time.

There are some aspects of concern regarding the IRMF implementation that one needs to note. Lowenthal (2009:5) cautions regarding the inter-relationship between the coordinating and departmental levels with the executive governance level. Furthermore, they argue that the intelligence agencies must not become involved with executive governance and policy formulation functions because it can create issues with agencies being politicised or influenced by policy-makers. Lowenthal (2009) illustrated this division as seen in the figure below.

POLICY VERSUS INTELLIGENCE: THE GREAT DIVIDE

One way to envision the distinction between policy and intelligence is to see them as two spheres of government activity that are separated by a semipermeable membrane. The membrane is semipermeable because policy makers can and do cross over into the intelligence sphere, but intelligence officials cannot cross over into the policy sphere.

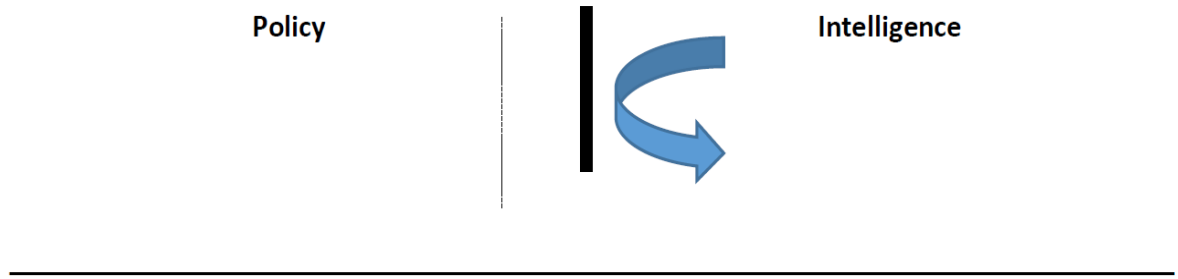


Figure 8: Policy versus intelligence: The great divide

Source: Modified from Lowenthal (2009:5)

Notwithstanding, Bracken (2008) argues from an RM perspective and indicates that intelligence agencies do not control their intelligence process environments. The intelligence cannot task any policy-maker on what to do or not do. Intelligence practitioners and managers need to understand and apply warnings from the bigger picture of uncertainty and risk. Their reporting needs to communicate a specific language that will inform the decision-maker of alternatives to handle the uncertainty with confidence. These decision-makers and executives should also understand that the intelligence agency forms part of an IRMF. This framework is necessary, as it ensures that warnings are not looked at in isolation and can be handled by other means. The framework developed within this research is based on other studies the investigated how organisations deal with uncertainty, with modern management theory as a director. Walsh (2011) believes that intelligence organisations dealing with the above concepts need to investigate some traditions which form the basis of IRMF development. Thus, this study will look into these traditions as described by Walsh (2011).

3.4 An Evolving Intelligence Risk Management Tradition

As discussed in Chapter Two regarding IRM in the traditional intelligence and national security environment, this study explores whether it is possible to argue an evolving IRM tradition. Walsh (2011:29) indicates that a tradition could be defined as *a set of beliefs, customs, practices, principles and accumulated experience handed down from earlier generations of intelligence practitioners that inform contemporary practice*. In addition, Walsh (2011:ix) questions leading economists and business leaders during their research regarding the 2008 global financial crisis. *He asked many business leaders both in Australia and overseas how the crisis came upon us so quickly? How, was*

it possible that with the sophistication of environmental scanning and budget forecasting models employed by developed economies, did this happen without anyone seeing it?

Furthermore, Walsh (2011) analyses these questions and the answers they obtained and came to one specific conclusion - that countries' intelligence frameworks need to change and be enhanced. Furthermore, they expanded these views and argued that a specific intelligence framework needs to be developed based on a historical traditional national security and policing environment. Walsh (2011:9) specifically based their views on defining national security intelligence as *intelligence collected, analysed and disseminated for decision-makers in support of the state's security*. These arguments provide a foundation from which IRM can be better understood, described, and viewed. Therefore, the question arises: how does one formulate traditional standards for IRM? In Chapter Two, it was argued that it is necessary to i) set vocabulary/language; ii) define intelligence (a very 'contentious' task) in the changing world; iii) understand the inter-relationship between intelligence, RM, and national security (that there are more asymmetric threats and new risks that exist); and iv) understand that intelligence processes have changed due to the new language, norms, cultures and approaches in the national security landscape. To articulate an IRM tradition, which is a new field of study, will force academics and practitioners to investigate different Social Science fields of study (for example, business studies, psychology, strategic studies, environmental studies, RM studies, national security or economics) to obtain the necessary knowledge to make sense and improve the understanding of IRM.

In Chapter Two, intelligence was explored in order to define it as a specific process that shifted towards uncertainty and risk. Warner (2009) and Phythian and Gill's (2018) views and arguments were of great importance because they enhance some of the characteristics that Walsh (2011:9) refers to (surveillance, secrecy, and national security). Throughout history, intelligence and RM have developed to provide recommendations to policy/decision-makers to manage uncertainty and risk (threats) against the state. Walsh (2011:9) explicitly identified three characteristics that describe the intelligence tradition, namely *the security environment, secrecy, and surveillance*.

However, some researchers approach intelligence theoretically, arguing that more or fewer characteristics need to be highlighted. Intelligence and its definition have remained contested among academics and practitioners in the past 50 years. This dissertation will make use of Walsh's (2011) three characteristics, with new emphasises added from academics such as Warner (2009), Gill (2012), Phythian (2012), and Bay (2007) to give more clarity regarding IRM. These academics' understanding of intelligence changed the approach to the security environment in which intelligence frameworks function, and therefore, should be investigated and analysed.

3.4.1 The security environment

The first characteristic of an IRMF is the security environment, influenced by uncertainty and risk in the new approaches that intelligence agencies apply in the fast-changing world. This landscape can differ in some ways or be similar in others if approached from an intelligence perspective. The *raison d'être* of any framework used in the intelligence environment is to provide the policy/decision-maker with the necessary IRM product which supports their responsibilities to manage the security landscape. At their most fundamental level, these products will ensure that executives manage their risks in the operational environment and better know the external and internal threats and risks that can influence their security operations. Therefore, these executives should understand all related threats and risks of their specific field of responsibility. These can include terrorism, international crime and syndicates, corruption and fraud, as well as environmental risks that impact water, food, and energy security, amongst others. The role of the IRMF will be to provide plausible recommendations and products which will not only cover the security environment or the priorities of the decision-makers but must be broader to ensure the bigger picture is understood, as well as every possible risk and threat has been attended to. These intelligence agencies will also identify the necessary additional threats and risks that can impact the specific environment.

The priorities mentioned above will then influence the priorities of the agency's collection and analysis environment and processes. New technologies and systems drive these processes, and coordination methods will provide the necessary knowledge and understanding to the decision-makers regarding the whole spectrum of threats and risks that they weren't aware of when first planning. These methods have been used for 20 years within national security; however, agencies were hampered during implementation due to poor coordination, communication, and management. Likewise, Walsh (2011:30) argues that *through the generation of new intelligence systems and processes, autonomous from formal tasking and coordination mechanisms, the intelligence function can recalibrate decision-makers priorities, or better still warn about an emerging risk that the decision-maker does not know of*.

Security is still the primary goal that intelligence agencies try to achieve. Security provides the necessary safety net, reducing uncertainty or adequately managing risks. These security arrangements define the boundaries of IRM, which is different from other information gathered for public purposes. However, impenetrable security is not possible and can lead to poor social relationships. To this extent, Betts (1978:89) states that *the intractability of the inadequacy of intelligence, and its inseparability from mistakes in decisions, suggest one conclusion that is perhaps most outrageously fatalistic of all: disaster tolerance*. This study's approach, namely that human

security is more broadly defined than traditional national security, will extend our field of IRM to embrace the former paradigm.

In addition, Gill (2009:214) states that several essential concepts influence the security aspects of intelligence frameworks and processes. These concepts need to be considered in order to understand security in the intelligence environment. Firstly, intelligence exists due to competitors; there would be no need for intelligence without competitors because governments would not 'feel insecure'. Gill (2009:216) furthermore states that *competitors cover a wide range of potential adversaries in order not to limit intelligence to its traditional concern with international relations between states. A key element in the competition is the resistance by targets against attempts to gather information and exercise power against them. It is this phenomenon that gives rise to the need for counter-intelligence.*

Secondly, forewarning in an IRMF will ensure a core function of an intelligence agency, namely to anticipate, estimate or give plausible recommendations for future uncertainties or threats. Gill (2009:216-217) indicates that these activities may be enhanced to ensure that agencies cover more aspects than only forewarning. Furthermore, the author states that *however, once intelligence (as knowledge) is developed, there are a variety of uses to which it may be put. For example, after a violent attack, authorities will wish to investigate to establish the (domestic or foreign) perpetrators and, to that end, will seek to draw on what, if anything, was known beforehand as well as deploy investigative techniques that are, in effect, post hoc intelligence activities* (Gill, 2009:217). These aspects show that intelligence is about the security of the governmental environment and that counterintelligence is a security phenomenon significant in understanding and implementing security in the IRM environment.

Thirdly, threats, risks, and vulnerabilities are the most common way to view IRM as a *defensive* technic against perceived domestic and foreign threats, risks, and vulnerabilities. 'Threat and risk analyses' and security assessments are some of the most basic IRM products of these services, which they produce for their customers to make better-informed decisions in uncertainty.

Fourthly are opportunities; however, it does not provide the whole picture - even if defensive techniques are the primary form of protection. Foreign and domestic intelligence must be changed, coordinated, and developed to enhance IRM products, which need to inform the government about opportunities. These IRM products will advance national security, military, economic or political interests. Within this context, Gill (2009:217) states that *the offensive use of intelligence can be witnessed in various forms including propaganda, material support for oppositional groups abroad, or as the basis for physical intervention including undermining the counter-intelligence efforts of competitors*.

These concepts intend to enhance the intelligence agencies' activities (IRM) which are goal-seeking processes to change the current situation. These new changes to the intelligence processes and impact on IRMF as described by Gill (2009:216) *may just 'fail' in the sense of not obtaining needed information or preventing an attack or, even more seriously, may 'blowback' as in the case of the provision of stinger missiles to the Afghan mujahedin in the 1980s* by the USA and UK's intelligence agencies. This chapter will explore these concepts in the context of discussing the newly changed approach in an IRMF more broadly.

3.4.2 Secrecy

As argued in Chapter Two, secrecy is a very contentious aspect of intelligence studies. Academics and practitioners differ regarding the influence of secrecy in defining intelligence. To this extent, Walsh (2011:30-31) states that secret information is not the only information that determines intelligence, but a significant proportion – probably over 90% – of information collected is made up of open sources to disseminate intelligence. Historically, intelligence agencies' work and existence were kept secret from public scrutiny. According to Walsh (2011:30), *historically, though not always, in reality, intelligence has been defined by the ability to collect sensitive information without the target's knowledge. Secret intelligence collection is important for decision-makers to forewarn about a target or threat and its possible intentions*. These views do not change the fact that agencies have started relying more on open sources and liaison information. Agencies will have to change and manage the IRM processes to share intelligence with other entities that play a more specific and relevant role in the intelligence environment. The culture of these agencies must be focussed more on how to responsibly manage the 'need to know' (secrecy) principle in their environments to ensure better results.

It is not only secret information that plays a vital role in informing policy/decision-makers regarding imminent threats and risks. These agencies also created secret and closed intelligence systems to provide the executives with early warning or foreknowledge products. As Herman (1999:203-204) notes, *most intelligence agencies now conduct foreign liaison of some kind; indeed, access to bigger partners may be the main justification for some agencies in small powers. National intelligence systems are not self-sufficient. Intelligence on some subjects (international terrorism and nuclear proliferation now) has become a kind of international knowledge system, a partial and undeclared replica of open systems such as the World Meteorological Organisation. The result is a patchwork of bilateral and multilateral arrangements of all kinds and all degrees of intimacy. The patchwork is unusual in its secrecy but otherwise is not unlike the intergovernmental arrangements that have developed in other specialised areas.*

However, there is no doubt that transnational security threats' current scope and nature have resulted in more flexible and arguably networked approaches, requiring at least some cultural shift away from earlier hierarchical Cold War structures and attitudes of secrecy within contemporary intelligence agencies. Secrecy is still a fundamental characteristic of intelligence that ensures competitors remain unaware of targets; however, secrecy should not hinder agencies from providing 'in time' intelligence products to their client and, in so doing, ensure that the client can manage uncertainty properly – based on the provided threat and risk identification. As argued below, secrecy will have a big influence on the operational collection of intelligence work.

3.4.3 Surveillance

The third characteristic of the intelligence tradition is surveillance, which includes several related and interdependent activities, such as tasking, coordination, covert, collection, analysis, and decision-making support. Gill and Phythian (2006:29) explain that surveillance is a core concept of national security intelligence as *[it] helps generate knowledge in conditions of secrecy that can inform the formation and implementation of security policy; this is essentially a subset of the more general surveillance that constitutes contemporary governance*. However, Hilsman (1952:25) comments that *Intelligence on the one hand and policymaking and action on the other are separated physically, organisationally, chronologically, functionally, and by skills – separated in every possible way*. The question is whether this division of labour is a wise or even valid one. Hilsman (1952:42) furthermore states that *intelligence and policy-making in foreign affairs, if our working model has a point, it is that the need is not for separation of knowledge and action, but an integration of the two. In rationally conducted foreign affairs, the relationship of knowledge and action should be one of continuous interplay; knowledge and action should interact, should condition and control each other at every point.* This dissertation concurs with Gill (2006), Hilsman (1952), and Phythian (2006) - that intelligence does not only provide knowledge but also provides action by policy/decision-makers.

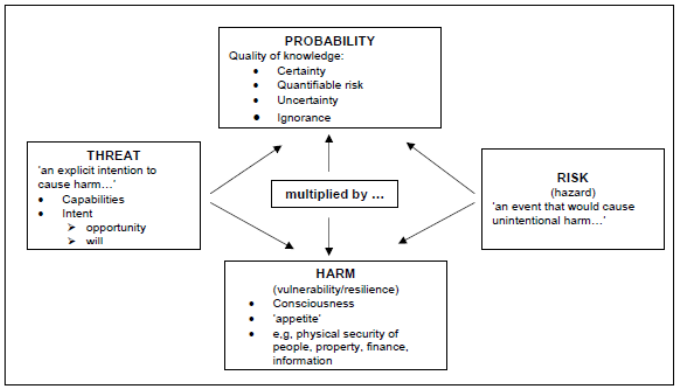
Whilst this understanding could provide the necessary security for liberal democracies, in non-democratic ('counterintelligence') regimes, these aspects of intelligence are directed to ensure the defence of a specific regime and against its people. Thus, in non-democracies, national security is known to be a cover for the enhancement of power by the regime. These actions serve the interests of a few groups or elites, not that of the nation.

These developments have changed agencies' approaches to and application of surveillance. The global threat and risk changes increased the use of surveillance by government agencies and the private sector. These changes tempted Gill and Phythian (2018) to enhance their definition of surveillance beyond national security to include a multi-layered process. Notwithstanding these

changes, surveillance is still a common characteristic of all intelligence practices. Thus, both the private sector and governments worldwide spy and collect information on each other.

In summary, Gill (2012:209-210) depicted (Figure 9) approaches by intelligence agencies and private businesses to threat/risk assessments, as well as their attempts to produce IRM products based on the calculated probabilities multiplied by harm. The figure shows that there is a clear difference between threats and risks. Threats specifically cause harm, while risks unintentionally cause harm. This situation is of great importance in the IRM process. As also supported by this study in a multi-layer IRM process, these aspects will influence practitioners and management to ensure proper communication between structures, to prevent both threats and risks.

Furthermore, there is a confined view that risk is only used in intelligence agencies to determine the risks and safety aspects involved during operations for their agents or informants. The World Commission also supplements these approaches through the Ethics of Scientific Knowledge and Technology's (COMEST, 2005:29) understanding, described as follows: *Generally, four types of practical decision problems can be distinguished: a decision under certainty; a decision under risk; a decision under uncertainty; and a decision under ignorance. In the case of certainty, we know the outcomes of different choices, and the only challenge is to be clear about one's preferences. In the case of risk, we know the outcomes (benefits and adverse effects) and the probability of various outcomes. In the case of uncertainty, we know the possible outcomes but have no objective ground to estimate their probability. In the case of ignorance, we do not even know what adverse effects to anticipate, or we do not know their magnitude or relevance and have no clue of their probability.* In addition, Gill (2012:210) postulates that *traditional risk analysis has operated mainly in the first two conditions (certainty and quantifiable risk), whereas intelligence has always operated primarily in the other two (ignorance and uncertainty). The overlap occurs in 'uncertainty' where quantification is impossible, and the precautionary principle may come into effect. 'Harm' summarises the variety of factors involved in estimating potential damage, including perceptions of vulnerability, resilience, and the 'appetite' for risk.*



Source: Reproduced from Gill (2012:210)

Figure 9: Threat, risk, probability and harm

Nonetheless, the above arguments show that the traditional cornerstone of intelligence (surveillance) needs to be applied in all possible ways, including physical, technical, or electronic surveillance methods. Therefore, from an IRM perspective, this study postulates that it will strengthen the impact on the traditional areas of national security and policing intelligence. These changes to surveillance will provide adequate forewarning and relevant knowledge of all threats, risks, and vulnerabilities, and more so, identify opportunities. These IRM products need to be communicated to all the different role-players identified as relevant clients when disseminated. Furthermore, this could affect the external and internal environment, which could ensure a much safer and more secure environment. The above characteristics will provide the necessary knowledge and understanding to determine an effective IRMF.

3.5 What Determines a Good Intelligence Risk Management Framework?

This study postulates the notion that an IRMF requires specific aspects to be effective. To this extent, Walsh (2011:90-129) describes several essential aspects to create or implement a proper intelligence framework. These aspects can be used by any country or institution worldwide and are summarised in the paragraphs that follow.

Firstly, a framework must be *mandated* by the government or executives. This will ensure that everybody is on board and there is 'buy-in' from the highest governance and executive members to ensure the successful implementation of this framework.

Secondly, a project of this nature should be planned, created, and implemented through sound *project management* principles. Walsh (2011:109) indicates that when interviewing those involved with intelligence frameworks in the USA, Canada, UK, Australia, and New Zealand, they found success because project management was applied in the processes. Project management ensures that everybody knows what needs to be done, the necessary finances, good communication and timelines are followed, and professionally trained people are involved in implementation.

Thirdly, Walsh (2011:96) identified that these frameworks ensured that commanders in the policing framework *made better decisions* and reduced crime. These frameworks *also had the effect of making both intelligence staff and decision-makers more accountable*, specifically at the tactical, operational, and strategic levels. Furthermore, these frameworks seek to identify patterns and resolve problem areas more efficiently.

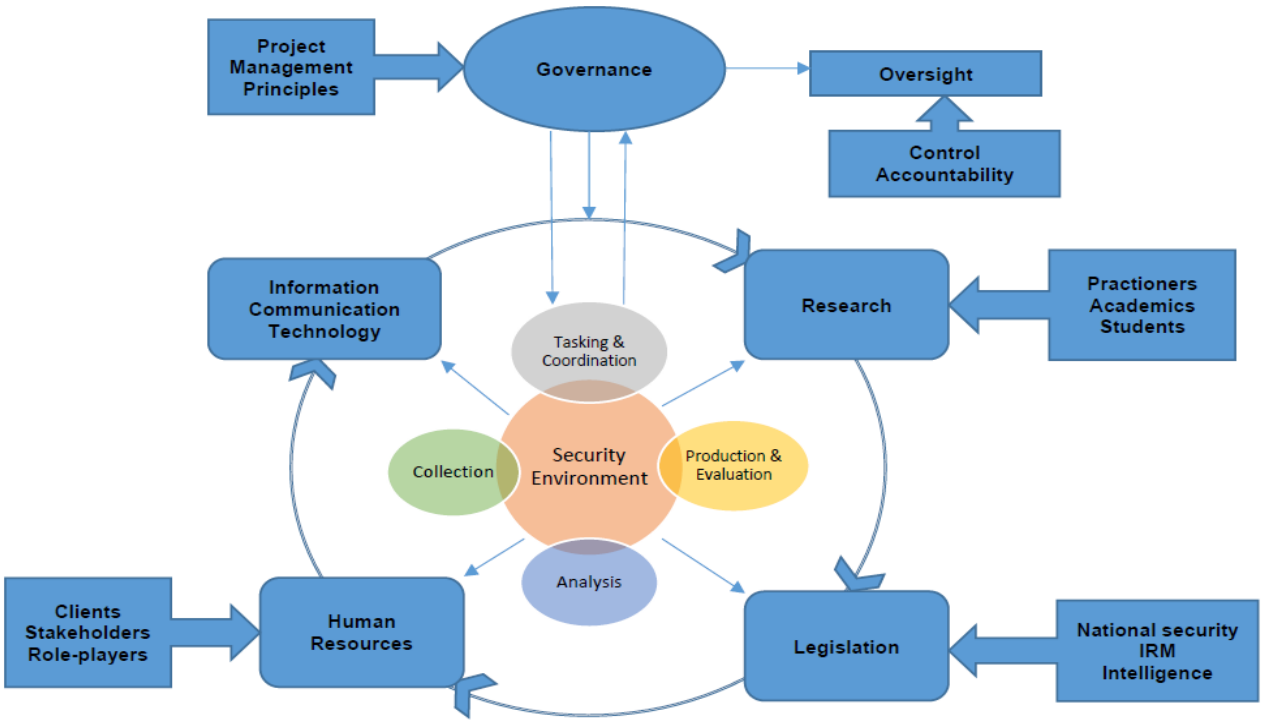
Fourthly, a framework will provide *proper structure and processes*. Furthermore, frameworks and carefully planned structuring will ensure creativity, but Walsh (2011:96-99) (through interviews) has

determined that it will provide creativity and *flexibility*. If the framework is correctly and consistently applied, it will provide better-integrated products which will influence strategic and tactical decision-making. This clearly shows that an IRMF can provide a more advanced option to agencies to coordinate intelligence risks and uncertainty over different levels of government (local, departmental, regional, national and international). These aspects will enhance management and provide the managers with the necessary opportunity to task and coordinate IRM throughout their business.

Fifthly, an IRMF will, according to Walsh (2011:105), provide *four pillars* from which the enhancement of the framework can function. The benefits of a framework include:

- *Better integrated intelligence products and services.*
- *Information/intelligence storage, retrieval, and exchange will be enhanced through new and updated technologies*
- *It enhances the priority setting, monitoring, and coordination of the intelligence risk processes.*
- *It will also provide needed professional development/education/training in intelligence-led operations.*

Sixth, Walsh (2011:148) argues that all frameworks had a *few variables* common to all intelligence frameworks *regardless of the specific context in which it is being implemented*. Intelligence, as described in Chapter Two *is a set of processes and products to support decision-making about the threats in the security environment*; this indicates that a good framework *needs to have both effective core intelligence processes and key enabling activities*. Walsh (2011:148-149) describes an intelligence framework from an engineering context. They view intelligence activities as the super-structure or intelligence cycle that rests on a very prominent substructure. This substructure comprises five key activities that influence the intelligence framework to ensure its efficiency. This includes governance (oversight), information communication technology, human resources, legislation and research. Likewise, other related perspectives influence a well-designed intelligence framework which will be investigated later in this study. This framework is depicted below.



Source: Adapted from Walsh (2008:148)

Figure 10: Components of an effective intelligence framework

3.6 Influence of Other Related Perspectives

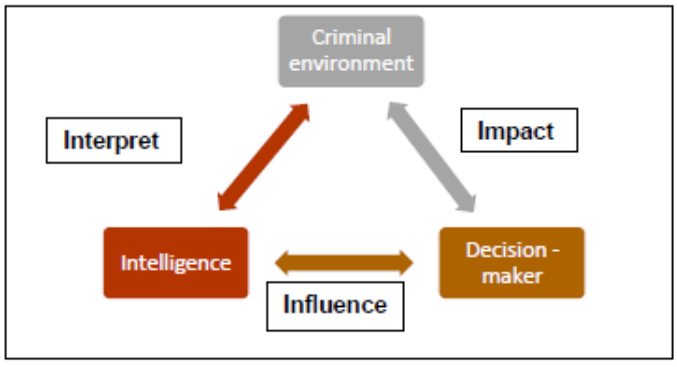
Other related perspectives can influence the development and implementation of an IRMF. Therefore, these perspectives need to be analysed and studied to ensure an intelligently designed and implemented IRMF. To this extent, Classen (2005:11) states that *It is generally accepted, when looking at intelligence* ***from a comparative perspective,*** *that the nature of a country's intelligence system, largely, reflects the nature of that society – its traditions, history, culture, and political system*. Furthermore, Godson (1988:2) explains that: *There are intelligence experiences throughout world history that are comparable, but that there are in diverse historical and cultural contexts important differences*. Therefore, it will be a grave mistake to think that an intelligence system that has evolved in one country and has withstood the test of time can successfully be duplicated in another country without further ado. Undoubtedly, we can learn from other experiences and elements can be adopted and integrated from other systems that consider our traditions, culture, and way of thinking. A new or restructured system should be given time to adapt and develop through natural evolution. Thus, the IRMF will give a comprehensive, workable system adapted for any country and provide some traditional aspects applied by most intelligence processes worldwide.

In addition, Bracken (2008:29) argues that intelligence agencies grow and become much larger, which influences their intelligence products *as large organisations get much more complex, there is a tendency toward high levels of specialisation. The number of departments increases, and so does the number of specialists. The legal department behaves like lawyers, the technology people like 'techies',*

and the marketing people like marketing people. A result is increased fragmentation at the level of the whole enterprise. A fascinating feature of many of the case studies of corporate disasters (Enron, WorldCom, Equitable Life Assurance, Arthur Andersen, and others) was the way people at the top were completely unaware of the state of affairs in their own companies.

Bracken's (2008:29) statements show that executives need to take note of growth and change their approaches accordingly, to ensure they attend to all the uncertainty and risk in their organisation. They must ensure good communication so that no silos are created due to specialisation during growth and change in their environment. These phenomena will influence the risk and uncertainty landscape of their institution.

In addition, perspectives such as the Ratcliffe 3-I model (Ratcliffe, 2008) can explain what intelligence does, namely interpret the environment and inform decision-making. These perspectives influence and bring some more clarity to the understanding during the conceptualising of an IRMF, which should be integrated and holistic. However, this study proposes the introduction of the phrase 'intelligence tradition' distilled down into only three characteristics of what is meant by the *business* of intelligence. However incomplete, the characteristics have, at the very least, been fundamental to defining what intelligence is, compared to other similar activities, such as research, data analysis, information collation, and report writing. The Ratcliffe 3-I model (2008:110), as relevant to the concept of assessment and management of risk, is depicted below.



Source: Reproduced from Ratcliffe (2008:110)

Figure 11: Ratcliffe's 3-I Model

3.7 Conceptualising an Intelligence Risk Management Framework

A conceptualised IRMF supports this research's suggested holistic intelligence process. This is also supported by Walsh (2009:16), who claims: *This is unlikely to change shortly as national security intelligence agencies seek to balance secrecy, including their use of proactive intelligence collection, and targeting with greater legislative, political, judicial and public scrutiny*. Executive management control can be exercised directly or indirectly. Intelligence functions within military, civilian or law

enforcement agencies are usually supervised by sector-specific ministries or departments, such as defence, justice, or the interior. Autonomously operating intelligence services often fall under the direct control of the executive, through the President or prime minister's office or a joint executive body such as a national security advisory board. In the SSR backgrounder of the DCAF (2006) series on intelligence and security control arrangements, 'Intelligence Services' presents various institutional arrangements in a democracy that will influence the IRMF in these states. This conceptualised framework will ensure better governance, management, and control over intelligence and security services in a country. Furthermore, it will change the processes in these services/agencies to be applied in an IRMF process and not follow the traditional intelligence processes. This conceptualised IRMF is based on different trends which require more deliberation.

3.7.1 Executive and governance level

The executive and governance level in an IRMF will fulfil a significant role in ensuring success with implementing the specific new approach in the intelligence environment. This level must ensure that proper buy-in, good governance, communication, objectives setting, and priorities are complied with. An IRMF should provide the necessary intelligence regardless of whether these agencies' work has become more time-sensitive, complex, dangerous, and controversial. Through a meticulously designed IRMF, these agencies will support the necessary changes which will empower this executive/governance level with the following outcomes, as described by the Geneva Centre for the Democratic Control of Armed Forces (GCDCAF) (2006: 2-3):

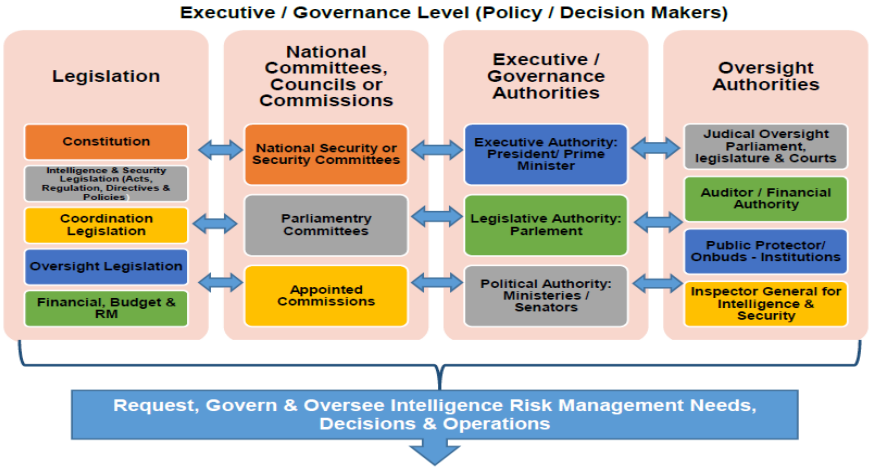
- *Effective decision- and policymaking is increasingly dependent upon early identification of problems, rapid assessment of the likely consequences of decisions and real-time monitoring of their implementation.*
- *With changes in the strategic environment, there has been an increase in intelligence consumers, both domestic and foreign. Their needs vary enormously.*
- *Only if top executive decisions- and policy-makers are well informed can they provide the necessary guidance to intelligence services and make sound judgments on policy.*
- *The work of intelligence services in some countries is being hampered by a crisis of confidence in their efficiency and commitment to democratic oversight. The problem is exacerbated where the public is not sufficiently informed about the activities of the intelligence services and the methods for controlling them.*

Therefore, four particular components are needed to ensure this level complies with and supports the national security intelligence environment. These components are postulated as legislation, national committees, executive, and oversight. Their specific roles, functions, responsibilities, accountabilities, and managerial positions in the IRMF are depicted by this study in Figure 12 below. The four

components are identified as the most critical aspects of an intelligence framework in liberal democracies, which ensure proper governance, management, control, and oversight.

Firstly, the ***legislation*** component is described by the GCDCAF (2015) as the institutions or units in government that are responsible for legislating security matters. Through legislator scrutiny, amendments, and approval, these government components will ensure that legal control and framework oversight of intelligence agencies take place. They will oversee the performance of these agencies' legal implementation of all security-related policies, investigate these agencies' activities, and provide opportunities for political parties and the public to deliberate the legal framework (including international law) and activities of this security sector.

Secondly, the **National Committees, Councils, or Commissions** component are state bodies appointed by the President or prime minister to direct and oversee the intelligence/security sector of government. These committees, councils, or commissions are legally and politically independent with a legal mandate for their work. These state bodies are National Security Council (NSC); the South African Human Rights Commission (SAHRC); anti-corruption commissions, supreme audit offices, and customary or traditional authorities. These bodies can receive complaints from political parties, organisations, or the general public, which must be investigated. They report on their findings and make recommendations in line with their legal mandates to the President, prime minister, or parliament. Furthermore, they provide the executive with the necessary information to give strategic direction to the security sector, parliament, and the intelligence coordinating and departmental levels.



Source: Researcher's construct

Figure 12: State institutions have specialised roles to play in democratic governance, control and oversight of intelligence & security agencies

In an IRMF, the role of the NSC has a vital function to ensure national security in a country. This council/committee, which the President or the deputy president usually chairs, is the central controlling body where all aspects of national security policy are developed, coordinated and implemented. Therefore, all products from an IRMF (whose primary goal is to enhance national security intelligence

products, a better and speedier early warning, and quality knowledge products) will be directed by this council/committee. The NSC has a decision-making or advisory capacity; this depends on the government's use of this type of council/committee. The DCAF (2010:4) states that this council/committee has the following primary activities to be successful in a country's national security environment:

- *acting as a body for ventilating different views on security issues and developing consensus positions;*
- *elaborating a strategic framework for dealing with current and emerging risks and threats, and structuring longer-term planning, including resource allocation;*
- *devising policy options and recommendations for the government on specific matters;*
- *coordinating the activity of government ministries and departments with a security role;*
- *taking the lead for the government in a state of emergency; and*
- *selecting individuals for high-level appointments in the security sector.*

The third component, the **executive/governance authorities,** has various sub-components. Each of the sub-components has particular functions regarding the governance of the security sector, which will influence the IRMF. The **executive authority** (head of government and/or state, deputy) has the final say on security policy, appointment of commissions, council members, and heads of state bodies and departments. The head of state approves all legislation and ensures good control through executive management and administration. In an IRMF, the head will be held accountable for all executive decisions regarding the IC by the elected parliament or legislature. In a democratic state, regular elections will determine if the regime has complied with the public's wishes; alternatively, through judicial review, media scrutiny, and the public's consultation and debate, the executive's actions will be judged. The appointed Parliamentary audit or security committee or commission will also evaluate the implementation and application of the IRMF by the executive and report to Parliament.

The second sub-component of the executive/governance level is **Parliament or legislature.** Through specific committees (representatives from all parties in Parliament and identified specialists from government departments), Parliament will legislate security matters. They will scrutinise, amend and approve all legislation and budgets for the intelligence sector. Furthermore, they will oversee the sector's performance in implementing security legislation, policy, regulation, and directives. They will also investigate the intelligence agencies' activities (surveillance, analysis, counterintelligence), review all year/audit and RM reports findings, and adhere to civil society input on security affairs.

The third subcomponent is the **ministries or senator's** offices which need to manage the coordinators and departmental environment of the IRMF. Primarily, these offices manage the day-to-

day administration, organisation (structuring and organisational design) and budget of the departments for which they are responsible on behalf of the executive/governance level. These offices need to provide the necessary resources and strategic direction at the departmental level to implement the legislation and policies. The ministries are the first line of defence/control to ensure that the intelligence departments are not pulled into the political arena. As Lowenthal (2009:5) explains, intelligence and policy are *two spheres of government activity that are separated by a semipermeable membrane. The membrane is semipermeable because policy-makers can and do cross over into the intelligence sphere, but intelligence officials cannot cross over into the policy sphere*.

The fourth component of this level includes **oversight authorities,** which should ensure that the intelligence agencies comply with the country's 'rules' and legislative framework. Oversight authorities normally do not have controlling powers over the environment they oversee. They focus on whether all codes are obeyed, and whether intelligence agencies do not misuse their surveillance power against their targets (groups or individuals). Oversight functions can be undertaken by state bodies legislated by the executive/governance structures and, as stated by DCAF (2017:2-3), *by senior management of the intelligence agencies, who provide internal control. Independent oversight may be conducted by ombuds institutions and supreme audit institutions, while civil society and the media generally guarantee public, or informal, oversight*. For these authorities to be successful, some essential aspects need to be granted which provide them with access, independence, discretion, and authority. However, these aspects do not ensure that government work will be challenge-free.

As a traditional characteristic of intelligence agencies, secrecy in oversight places some challenges on authorities. The independence of these authorities is crucial to provide them with the necessary access to sensitive information through legislation. These members need to be vetted to the highest security status to ensure their access. However, some arrangements and legal mandates will overcome secrecy and security applicable to intelligence agencies. These intelligence agencies have independent authority and regularly make decisions with no oversight, since overseeing all decisions can be an arduous task. Therefore, intelligence agencies should ensure that, through policies, standard operational procedures, and codes, practitioners act professionally and ethically and obey legislative frameworks and the rule of law.

The secrecy and security regarding intelligence agencies' work and political influence on these processes place intelligence practitioners under pressure to comply. Nevertheless, the intelligence members need some protection from oversight authorities due to the political leaders' agendas and their claims of plausible deniability when things go wrong. These authorities can provide the necessary support in these situations due to their independence and mandates.

The DCAF (2017:5) states that *exaggerated threat perceptions in national security assessments had happened in the past. These perceived threats to national security can be used to justify actions that may be disproportionate to the threat and damage to the principles of democratic governance, human rights and the rule of law.* These authorities can successfully prevent these aspects through high professionalism, independence, and oversight work effectively.

However, whilst these aspects will ensure that intelligence analysts do not over or under-assess/estimate the threats in question, the change in global threats, international cooperation, and joint operations beyond their borders create a severe challenge for these authorities whose mandates and legal authority do not cover these operations. DCAF (2017:5) proposes that in these operational plans and agreements, one must *Define the scope and nature of international cooperation. This can prevent abuses and bolster the credibility of national intelligence services (NIS*).

These aspects mentioned above will ensure that an IRMF can be adequately implemented, followed and controlled. It will also provide the necessary feedback to the executive regarding the status of the intelligence environment and compliance with national objectives. Gill (2012:217) states that *the objective of intelligence oversight is to increase both its efficacy and propriety. In terms of our 'probability' continuum, the object of intelligence is to shift the state of knowledge from ignorance towards certainty or, as practitioners would say, 'truth'. This is not just to assess the 'threat at hand' but also explore other possibilities beyond security threats.*

In addition, Walsh (2011:132–140) determines that an adequately designed IRMF will provide the necessary strengths to the framework's inner workings to withstand the fast-changing world and new threats that governments face. During their research, Walsh (2011) focused on these strengths to evaluate the different frameworks in the five countries they investigated (New Zealand, USA, UK, Canada, and Australia) to determine the best arrangement of an intelligence framework for policing. *Firstly*, the frameworks that provided a political and legal foundation ensured the executives' properly implemented those frameworks with the most successful and speedy rollout, for different policing structures in the countries. These frameworks were also supported with the necessary resources to implement technology and budgets successfully. The executives and oversight authorities were involved, and standards and doctrine could also be developed for the integrated frameworks. *Secondly*, because of the integration of the frameworks, the frameworks did not only focus on some aspects of the intelligence processes but rather included all structures, processes, and products. These influences broadened the use of intelligence in policing, specifically in the UK. These processes further enhanced intelligence tasking and provided police managers and analysts with guidance on better integrating intelligence into decision-making. *Thirdly*, these frameworks focused the users on

the framework's outputs. If these frameworks could not deliver on the needs of the decision-makers, they would be vulnerable to receiving no support and help from the executive, which could lead to total mistrust by the users. *Fourthly*, these frameworks' support and integration provided a standardised network and database for the users. The framework also ensured better cooperation and liaison between different agencies and users. The core users began supporting other police units in the specific areas in which they were involved. These other police units, in some instances, did not have access to the entire framework. The framework lifted the culture of cooperation and support in the intelligence environment. *Finally*, the frameworks also enhanced the professional development of individual members (managers and analysts) as they supported these developments. Any framework's success is determined by how change management is applied, including the training of members in new applications and methods. Thus, Walsh (2011:137) summarises the impact of the frameworks as o*ther important issues that come under the remit of governance are the development of core components of the intelligence framework, such as effective strategic and tactical tasking and coordination arrangements and forging effective organisational (cultural) change management to ensure the new framework is implemented successfully. Unsurprisingly, effective governance requires strong executive leadership, both to conceptualise and project manage the suite of changes required to implement the new framework and then to review and evaluate the doctrine systems and processes that underpin the core components of the framework.*

Flowing from the executive and governance level is the coordination of the IRMF intelligence and work. This has been identified by some reports on intelligence as the main factor for intelligence failures worldwide.

3.7.2 Coordination level

In general, intelligence services – except where their sensitive functions make this impossible or unwise – need to become more like other governmental services in their attitude toward transparency, accountability, and engagement with the public. In a technical report, Hannah, O'Brien, and Rathmell (2005:35) state that *by ensuring central coordination, the government can ensure that individual agencies do not overlap, become involved in rivalries, and ensure complementary collection and analysis paths are followed*. The following figure indicates the aspects that need to be coordinated by states in the modern era by intelligence coordinators.

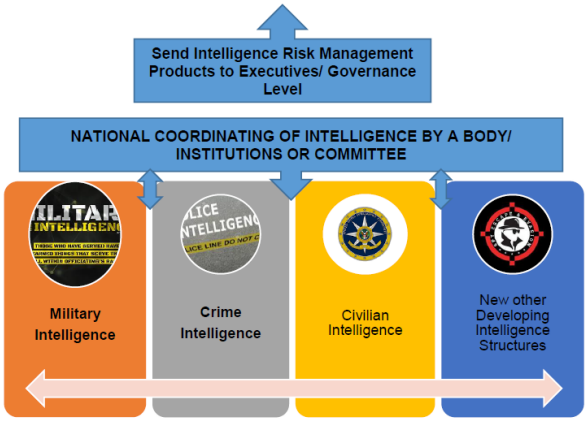


Figure 13: Coordination level in an IRMF

Source: Author's construct

These coordinators should ensure that all role-players in the intelligence environment are properly overseen to control all aspects of their secret and secured activities to collect intelligence. Furthermore, this body will ensure good cooperation, liaison, and clear legislative lines of accountability for their mandates and responsibilities in intelligence processes. This body will ensure that all national risk intelligence products are jointly coordinated between the necessary role-players, thus enhancing the products, ensuring that no duplication takes place and that the proper line of communication to the policy or decision-makers is followed at all times. Furthermore, this will ensure that policies or decision-makers will not be confused or receive products that do not cover all the inputs from all intelligence service providers.

Notwithstanding, Walsh (2011) explained the abovementioned aspects to compare the USA and UK arrangements regarding coordination. In both these countries, it was apparent that it has been a great challenge to coordinate intelligence, specifically national products, between the different agencies due to competition and lack of coordination. The most significant part of the budget in the USA was allocated to the military, and the CIA controlled the directorship. These aspects were indicated through the commission's 9/11 (2004) reports, and Silberman-Robb's (2005) reports. Therefore, the reform recommendation, specifically in the USA, was legislated in the 2004 Intelligence Reform and Terrorist Prevention Act, which gave more powers to the ODNI over the 16 intelligence agencies in the USA. There is no proof that these arrangements benefited the USA intelligence coordinating environment. All the UK and USA commission reports regarding 9/11, 7/7, and the Iraqi invasion of both these countries identified that coordination was an essential aspect of intelligence that failed.

Walsh (2011) furthermore used the Hendra Virus outbreak in Australia to enhance his views regarding coordination between agencies. In these biosecurity arrangements, it was found that the different agencies were not cooperating, influencing the connection between various experts. In the Australian case, more non-intelligence departments needed to play a leading role in containing the outbreak.

Walsh (2011:55) reviewed the Beale (2008) report and referred to Prowse *et al.'s* (2009) views regarding handling the situation in the Australian environment: *there needed to be better coordination and integration of expertise between those working on the virus, including wildlife biologists, vets, and human disease specialists*. The Beale (2008) report is noteworthy in advocating Australia's moving away from a traditional isolationist defensive quarantine approach that tolerates no risk to a more realistic one in the age of globalisation, which promotes an RM approach pre-border, border and post-border. Beale (2008) was also noteworthy in recommending the development of one supra institution that would pull together disparate agencies responsible for biosecurity. The report, however, makes a scant reference to the role of intelligence in promoting better RM of biosecurity, and there is only one reference to a new national biosecurity authority needing to work collaboratively with other relevant portfolios, including police and intelligence agencies. As mentioned and described by Walsh (2011), these case studies clearly show that intelligence and departmental coordination are needed to ensure more efficient and cost-effective measures.

Without a consistent strategic direction, the tasking and coordination of intelligence capabilities cannot be optimised. In today's security environment, intelligence services have to work more closely with other national security services. The former is especially challenging for larger countries with multiple intelligence services, though smaller countries usually also have multiple actors with intelligence-related functions, thus needing optimal cooperation. Central intelligence mechanisms consist of officials responsible for coordinating national intelligence estimates at or near the cabinet level in most countries. Intelligence coordination can be supplemented by ensuring that services have access to the same databases, documents and frequent contacts between agencies working on similar issues.

Furthermore, the increasing need for intelligence services to monitor transnational issues from a domestic scope (such as international terrorism and organised crime) requires a renewed emphasis on cooperation with other national security forces. In most democracies, intelligence services have restricted powers in domestic matters (searches, seizures, and communications monitoring). Thus, they are required to cooperate with other security forces at all levels of government such as the police, military, gendarmerie or 'constabulary' forces, national and border guards, and customs agencies.

In addition, elements of government not traditionally associated with security issues, such as ministries of finance, energy, trade, agriculture, health, and other groups, increasingly cooperate with intelligence agencies. In some cases, intelligence analyses can benefit from the expertise and experience of other government departments, while the latter can benefit from the expertise of the intelligence agencies in their activities. National coordination can be supported by measures such as:

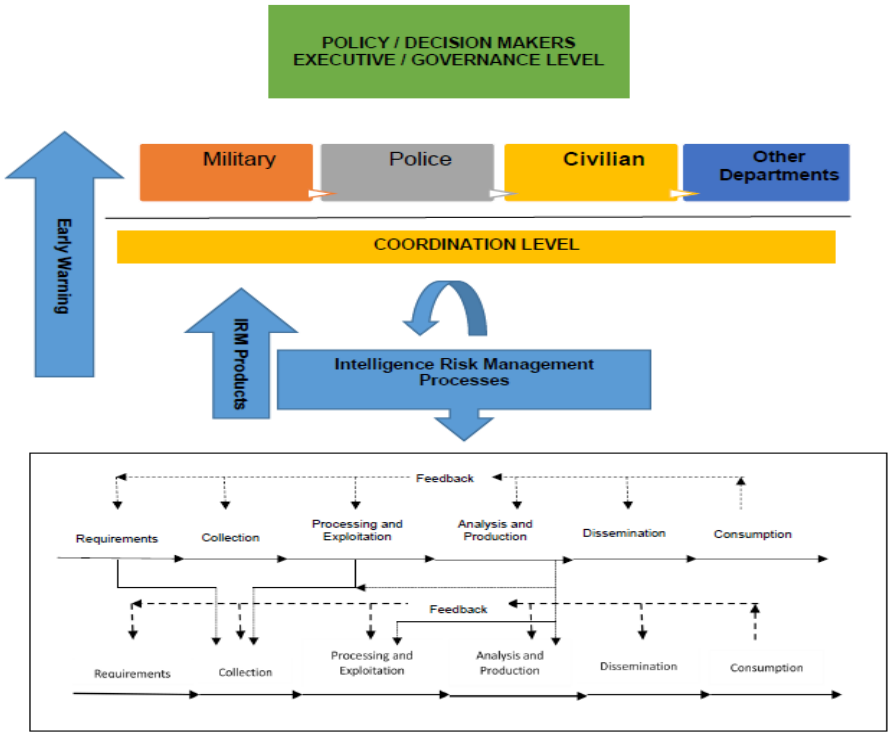
- Policy and emergency coordinating mechanisms, such as committees or working groups, operating on a permanent or ad hoc basis;

- Staff exchanges to provide liaison and channel communication and cooperation;
- Special, permanent inter-agency coordinating units to address specific issues such as counterterrorism or drug smuggling; and
- 'Situation rooms' to handle emergencies.

Therefore, a coordination body/committee or unit should be adequately legislated and should be appointed by the highest authority of government. This should include all government role-players (even in non-intelligence departments) and set properly formulated standards which control intelligence work in the IRM environment. These arrangements will ensure that the departmental level will provide the necessary IRM products, which will be analysed further below.

3.7.3 Departmental/Institutional level

The departmental level of the IRMF is the most critical level in ensuring that national IRM priorities can be achieved. Unfortunately, intelligence agencies are so set in their work that any new approaches will be faced with resistance. This study depicts this level in a conceptualised IRMF as follows:



Source: Author's construct

Figure 14: Departmental level in an IRMF

The figure above shows the new departmental approach in a conceptualised IRMF, which will be described further in this sub-section. Intelligence agencies need to change the method through which

they collect the necessary data/information provided for the IRM process. There are four main areas where the intelligence services need to adjust their approaches:

- Information collection and utilisation;
- National coordination and cooperation among intelligence services and with other security sector actors;
- Information sharing with international organisations and other countries; and
- Public acceptability and accountability.

Walsh (2011:31) correctly explains intelligence agencies' change to remain relevant in the modern world: *at the very least, traditional intelligence agencies are having to adapt their cultures of secrecy to work more effectively with new tiers of government and non-government agencies, which are themselves increasingly becoming part of national intelligence communities*. The figure above clearly indicates that these aspects are essential to ensure the implementation of an IRMF. Agencies that accept that change is needed should happily include all other departments and institutions that can assist them to obtain the necessary information and data (knowledge) to analyse these processes and provide the necessary intelligence. These changes will ensure that intelligence services and responsible executives can enhance public accountability and acceptability. Furthermore, these agencies need to ensure that two aspects, in particular, are enhanced. Firstly, all intelligence practitioners must have the necessary professional qualifications and receive training that is based on professional ethics and norms. Secondly, there should be a proper balance between secrecy and transparency in the change intelligence processes. Furthermore, the media, non-governmental organisations, and the general public need to be informed – and need to inform themselves – about the activities of the intelligence services and be able to do so without fear of sanction.

As already explained by this study and likewise explained by DCAF (2017:2), *the primary task of all intelligence agencies/services is to provide governments with credible intelligence (information) about possible threats, risks, vulnerabilities and opportunities to the state and its population* [own emphasis added]. Intelligence services should focus on the security environment, including emerging problems, threats to national interests, risks, and opportunities. DCAF (2017:2) defines these tasks of intelligence agencies/services to provide political decision-makers with the necessary analyses:

- *Define national interests;*
- *Develop coherent national security and military strategies and adequate security policy;*
- *Determine the mission, doctrine, and strategies of the armed forces and other security institutions;*
- *Prepare for and respond to national crises;*
- *Prepare for and prevent threats to the state and its population*.

The above changes will force agencies to formulate proper standards and doctrines regarding the securing of their processes and operations. Counterintelligence processes must be secured, updated and enhanced. Intelligence changes can include updates to policies, regulations, and standards. These security arrangements must ensure that the country is protected against espionage, terrorism, subversion, information and electronic data compromise, or sabotage by foreign and domestic advisories, political groups, intelligence sources/informants, and methods.

Furthermore, these agencies/services (as projected in Figures 10 and 11 above) need to work from the premise that the security environment on which they focus forms the central basis of the IRMF. The framework is designed around this focal point to provide the necessary IRM products. Therefore, this study postulates its arguments that intelligence agencies need to change their intelligence processes to a multi-layered process that will ensure integration and a holistic approach. The process is described by Lowenthal (2009:67) as *any one intelligence process issues likely arise (the need for more collection, uncertainties in processing, results of analysis, changing requirements) that cause a second or even third IRM process to take place. Ultimately, one could repeat the process lines repeatedly to portray continuing changes in any of the various parts of the process and the fact that policy issues are rarely resolved in a single neat cycle. It gives a much better sense of how the intelligence process operates in reality. The process is, therefore, linear, circular, and open-ended all at the same time.*

In this multi-layered process, there will be two actions taking place simultaneously. An intelligence process and an RM process will run parallel to each other, which inter-relate through good governance, management, communication, teamwork, and training in new methods and techniques of the IRMF. Within this context, Figures 10, 11, and 14 clearly support Walsh (2011), Ratcliffe (2003), and Lowenthal's (2009) arguments. At the centre of an IRMF is the security environment, and there is a particular IRM process based on the influence of this centric concept. It displays an integrated and holistic process that must be applied in a multi-layer faction to provide better IRM products. This multi-layered process feeds into the coordination level, which sends intelligence products to the executive and governance levels for policy/decision-making. This shows that Ratcliffe's (2003) module significantly impacts the changing security environment. These methods and techniques need to be standardised by the intelligence environment. Likewise, Bracken (2020:6) emphasises that in *the IC, there may be tremendous variation in the way risks are monitored, assessed, and managed across different departments. If the organisation's work is loosely coupled, this may be acceptable if one part does or does not affect the other. However, the trend in intelligence is for tighter coupling. This presents big problems if a risk assessment is conducted differently by the relevant divisions/departments/structures of government.* For this process to be correctly implemented, the

role-players' responsibilities need to be specified and summarised to understand their importance better.

3.8 Executive Management and Other Role-players Responsibilities in the Intelligence Risk Management Framework

This study will summarise and specify the different role-players in the IRMF based on democratic political control that includes civilian control, the rule of law, and respect for human rights. Within this conceptualised framework, good governance is provided through good oversight, control, and accountability by internal and external supervision of the intelligence environment. These concepts are controlled by providing clear responsibilities, a transparent process, and accountability to the public. A range of departments, structures, and executive role-players are involved in management and oversight. These role-players' responsibilities are summarised in the table below.

Table 7: Different role-players' responsibilities in an IRMF

Level	Role-players	Responsibilities
Executive/Governance	President/Prime Minister/Head of State	**The executive** (head of government and/or state) has the final say (approval) on security policy and controls, leads/chairs the NSCs or advisers (DCAF, Security Sector, 2015:4-5).
	Parliament/Parliamentary Committees/Appointed Commissions	The **Parliament or legislature** and its specialised committees legislate on security matters; scrutinise, amend and approve budgets for the security sector. Can also investigate the activities of the security forces when complaints are received (DCAF, Security Sector 2015:4-5).
	Ministries/senators	**Government ministries/senators** manage the administration, organisation, budget and provide the necessary resources to implement policy (DCAF, Security Sector, 2015:4-5).
	NSC or Security Committees	Whether an **NSC** performs a decision-making or advisory role, it tends to be involved in the following activities: ventilating different views on security issues; elaborating a strategic framework for dealing with current and emerging risks and threats; coordinating the activity of government ministries; taking the lead for the government in a state of emergency; selecting and recommending individuals for high-level appointments in the security sector (DCAF, NSC 11/2010:4).
	Justice authorities/Legislation units	**Justice authorities** play a role in security sector oversight by ensuring the security forces uphold domestic and international law; supervising the use of special powers about the legality of warrants, investigations, surveillance methods, or searches; holding security personnel accountable for violating the law; ensuring that security policy and the actions conform to the established norms of constitutional order; test the legality of new laws or policies for the security clusters (DCAF, Security Sector, 2015:4-5).
	Oversight authorities	**Special statutory institutions** receive public complaints and investigate, report on, and sometimes make binding recommendations about issues specific to their mandates (DCAF, Security Sector, 2015:4-5).
Coordination	Coordinator/Institutions/Unit	**Coordinator or unit needs** to coordinate all activities of intelligence and security sector actors to ensure**:** National coordination and cooperation among intelligence services and with other security sector actors; information sharing with international organisations and other countries;
	Departmental representatives	The **heads or representatives** of services need to ensure proper coordination and cooperation between these different institutions to enhance the joint focus on the security

Level	Role-players	Responsibilities
		environment through their operations. This will enhance the intelligence products to inform the executive/governance levels; furthermore, it will ensure the successful implementation of the national IRMF.
Departmental	Management	Internal control works through effective **management** to: Coordinate the process for assigning, reporting on, and evaluating all intelligence activities as well as staff performance; issue guidance for intelligence staff and ensure adherence to codes of conduct, regulations, legal standards, and professional ethics; identify and correct minor infractions while ensuring major infractions are appropriately dealt with by the justice system or higher institutions of oversight, as appropriate (DCAF, Intelligence Oversight, 2017:6).
	Practitioners	**Practitioners** need to cooperate and comply with challenges due to global changes in intelligence processes by implementing the following: deciding in which domains to rely on open sources and existing methods of collection, and in which to develop new capacities, involves developing new methods of exchanging and protecting data as cooperation among intelligence agencies increases (DCAF, Contemporary Challenges for the IC 03/2006:3)

Source: Author's construct and data obtain from DCAF (2006-2017)

3.9 Conclusion

In summary, this chapter attempted to conceptualise an IRMF based on the theories, definitions, and concepts described in Chapter Two. Chapter Two clearly stated that a meta-theoretical approach to understanding intelligence, RM, and national security will ensure that the new approach in intelligence work leans towards the IRM process. This new approach will ensure that the following can be achieved:

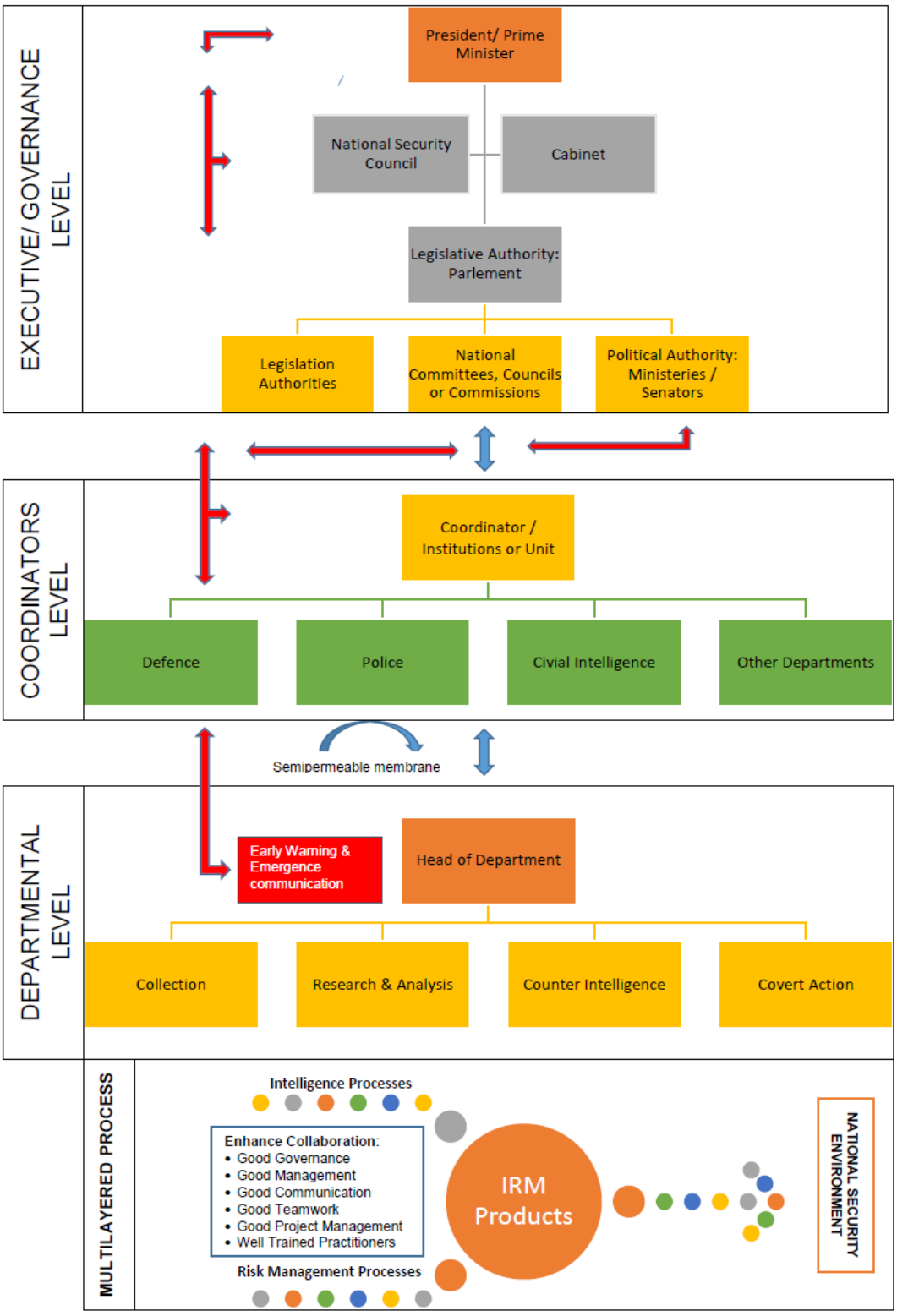
- A standardised vocabulary/language and knowledge;
- Good objectives and purpose for intelligence services;
- The necessary changes to the intelligence processes through new technologies, methods, and techniques;
- That intelligence agencies will make use of different Social Sciences findings and methodologies;
- That failures of intelligence can be prevented if RM principles are used; and
- That national security cannot be approached from the traditional perspective and that there should be a focus on widened human security aspects.

The conceptualised IRMF, being applied on three distinct levels (executive/governance, coordination, and departmental), should be inter-related to ensure success. Therefore, this IRMF will ensure good governance, management, communication, teamwork, project management, and well-trained practitioners. These aspects will also provide the necessary IRM products to inform the policy/decision-makers on the necessary intelligence to make informed decisions.

Figure 15 below shows the conceptualised IRMF functioning in a democratic state. It clearly shows that the IRMF should comply with the following essential aspects to be successfully implemented in a state:

- Each role-player will act in the framework at a specific level;
- There are specific communication lines that need to be followed to ensure coordination on each level;
- There should be an early warning and emergency communication channel, which will ensure that the government can take emergency or immediate action against any strategic surprises threatening the country's national security or interests;
- Coordination plays a significant role in the framework's success, and non-intelligence departments/institutions of government must be part of the coordination process;
- That the departmental level shows that it will not infringe on the executive/governance level and be influenced by the role-players to be politicised and to determine policy; and
- A multi-layered process that will be integrated and holistic in its approach, implemented through the departmental environment. This process will ensure that the inter-relationship of intelligence and RM will occur, which will deliver the necessary IRM products to the national security environment.

In conclusion, this conceptualised IRMF will ensure that this study can evaluate the SA intelligence framework to identify any shortcomings or amendments to be noted for a more efficient framework in the SA context. It will also allow an analysis of the framework's effectiveness in practice by analysing the instability within SA. It will give indications of the SA intelligence framework's strengths and shortfalls that can be overcome to ensure that the intelligence agency applies these recommendations and enhances its capabilities to the benefit of good governance and a safer country for all its people.



Source: Author's construct

Figure 15: Conceptualised IRMF

CHAPTER 4: INTELLIGENCE RISK MANAGEMENT IN THE SOUTH AFRICAN CONTEXT - IMPLEMENTING THE INTELLIGENCE RISK MANAGEMENT FRAMEWORK

…the idea of the future being different from the present is so repugnant to our conventional modes of thought and behaviour that we, most of us, offer a great resistance to acting on it in practice. (Keynes, 1937)

4.1 Introduction

Chapter Four builds on the previous chapter's conceptualising and construction of an IRMF. This component aims explicitly to contextualise the security and intelligence environment in SA and also analyses the level of/or lack of implementation of intelligence, RM, and national security. Furthermore, the chapter will also examine the historical trends in SA that influence the intelligence and IRMF processes. A brief historical analysis of the evolution of intelligence and RM will provide the necessary knowledge regarding these phenomena, current status and implementation in the SA context. Furthermore, it will contextualise the current state of affairs in the IC from an IRMF perspective and the challenges that the government faces.

Therefore, these phenomena' shortcomings and future developments can be explored and analysed to reconstruct an IRMF for SA. As mentioned, this chapter will examine intelligence and RM within the SA context. It will explain and describe how intelligence and RM developed from the end of apartheid to 2022 to analyse and evaluate its benefits and contribution.

The methodological approach in this part of the study is directed by analysing the SA intelligence framework through comparative analysis against the conceptualised IRMF of Chapter Three. These comparisons will then be evaluated against organisational structures, legislations, and available unclassified information. Examples will be provided in some instances of non-compliances by structures, individuals and groups which do not follow dual processes. Therefore, this chapter will follow qualitative research methodology, which includes descriptive and explanatory analysis flowing from the comparative analysis processes.

Chapter Four will further address the role of intelligence within the SA state apparatus. This brief historical analysis will show that how the two phenomena are implemented will be linked to the clarity and quality of the reporting of intelligence products that inform on national security, as there should be a balance between threat, risk, and vulnerability versus opportunity in the reports which advise the policy-maker/client on national security issues. Finally, the reconstruction of an IRMF within this chapter will enable its operationalisation within the SA context.

4.2 The evolution of intelligence, risk management, and national security

The three phenomena (intelligence, RM and national security) have their roots in embedded aspects, including espionage, the development of uncertainty from changes and probability theories, and the development of security for individuals to states. These aspects were captured in ancient archaeological excavations in parts of the world where ancient cities and emperors existed. As ancient civilisations and languages developed, these concepts became more understandable and analysed by academics and students. However, these three phenomena cannot be clearly defined by academics today and have brought about numerous discussions, arguments, and criticisms in intelligence studies.

The historical development of these phenomena is illustrated in Figure 16 below, showing that intelligence developed from espionage in ancient times into military intelligence, which dominated from the renaissance to World War (WW) II. In modern times (from WWII to the present), countries developed intelligence services/agencies to deliver national security intelligence products for the policy/decision-makers that would ensure a secure and safe environment for the public. RM as a phenomenon and management tool has only truly developed in the last 100 years within the sciences as a method of assisting governments and industries to survive threats, risks, and vulnerabilities in this unsecured world.

Additionally, national security as a phenomenon has only been viewed and analysed in its current understanding after WWII. Before this, national security was applied from the state's security and safety perspective. These states and leaders' national security views created an environment of conflict that forced states into wars to protect their territory and citizens. Thus, in modern times, there has been a realignment by academics, politicians and policy/decision-makers regarding how this national security phenomenon should be applied in a state, which includes more aspects of human security matters that influence the traditional perspective of national security.

TIME LINE	INTELLIGENCE DEVELOPMENT & CHANGE	RISK MANAGEMENT DEVELOPMENT & CHANGE	NATIONAL SECURITY DEVELOPMENT & CHANGE
Ancient Times 1st Century	Soothsayers Delphi Oracle Spies (HUMINT) Syrian Clay Tables Chanakya's Arthasastra Sun Tzu's Sunzi Bingfa Greek City States -couriers Roman Empire - Speculators & Frumentar Thucydides' Peloponnesian War	Soothsayers Babylonians – 3000BC – bottomry Greeks & Ohoenicians – 700BC - Bonds Gambling, through of bones Human oracles, priests, priestesses, and astrologers - predict the future. Mesopotamia, Sumeria, Egypt, Phoenicia - written language Thucydides (400 BC)- new penetrating realism	Individuals & deleing Greek City Physical security arrangements Overlapping authorities state system Phoenicians and early Hebrews – organised military forces Kingdoms – forces of men for offensive & defensive protection Overlapping authorities The principle of hierarchical subordination
Middle Ages 4th – 5th Century	Catholic Church Inquisition Crusades	Scientific instruments of the Egyptians, Greeks, Romans, Chinese or Indian Euclidian geometry, Arabic numerals, Hindu concept of zero Al-Khowar-izmi – algorithm Omar Khayyam - quatrains	Leviathan Territorial state system & monarchical form of government Chinese – Gunpowder Greeks & Rome well-disciplined military forces (armies) The Roman jurist Ulpian Churches (religious) and empires (political)
Renaissance 14th – 17th Century	Ambassadors/Diplomats Nation States - own intelligence Look-out Posts and Ciphers Machiavelli's The Prince Encryptions Dead drops	Leonardo Pisano (who introduced Arabic numerals) Luca Paccioli (double-entry bookkeeping) Girolamo Cardano (measuring the probability of dice) Exploration of probabilities Luca Paccioli, Blaise Pascal & Pierre de Frermat – theory of probability	Territorial state system & monarchical Europe – Gunpowder used in wars Peace of Westphalia (1648) Immanuel Kant (1724–1804) - Nation-states Jean-Jacques Rousseau's (1712–1778) Territorial sovereignty Religious differences – wars
Industrialisation 18th – 19th Century	Ministers and Secretaries Cardinal Richelieu John Turloe - Department of Intelligence French Revolution - Espionage Networks Deciphering - Black Chambers Mail Interception Wilhelm Stieber - Single Military Intelligence Agency Photographic Pictures Samuel Morse Bell, Watson - Telephone - Wiretapping Counter Intelligence	John Graunt (who calculated statistical tables) Daniel Bernoulli (the concept of utility) Jacob Bernoulli (the "law of large numbers") Abraham de Moivre (the "bell" curve and standard deviation) Thomas Bayes (statistical inference) Francis Galton (regression to the mean) Jeremy Bentham (the law of supply and demand)	Territorial state system Military force expanded with technically innovations. States created Police forces for domestic safety/ security The Age of Enlightenment French Revolution Sovereign territorial state Minimise religious conflict and wars
WW1 – WW2 Cold War Era 1914 - 1991	Real Time Intelligence HUMINT Military Intelligence Units Signal Intelligence Electronic Interceptions Integrated Intelligence Analysis & Assessment Intelligence Theory Intelligence Cycle Intelligence Community (Civilian, Military, Police) Covert Action Surveillance	Fayol – 1916 – security – management function Development of Risk management after WW2 as concept in the USA To manage insurable and uninsurable risk – 1970's to 80's Beginning of the development – International & national standards, regulations & codes 1975 – 1979 SA RM Association 1986 – SARIMA formed in SA 1990 – Society of RM formed in SA	Modern state - sovereign territorial state National security – traditional approach Wars - ideological ones (Capitalist West and the communist East) United Nations – founded on 24 October 1945
Morden Era 1991 - Present	Strategic Intelligence. Intelligence Liaison Economic Espionage Open Source Democratisation of Intelligence Sophisticated Intelligence Development by Non-State Actors Cyber espionage & attacks	Operational and liquidity risk management - 1990s Basel Capital Accord 1 (1988), 2 (2004), 3 (2010), 4(2017) Australia and New Zealand publishes the first Risk Management Standard, AS/NZS 4360:1995 South Africa King: 1 (1994), 2 (2002), 3 (2009) & 4 (2016)	Nation State Human security Rapped development of private security industry Globalisation Emerging technological revolution

ESPIONAGE

MILITARY INTELLIGENCE

INTELLIGENCE

RAW DATA/ STORY TELLING'S

INFORMATION/ KNOWLEDGE

INTELLIGENCE (DOMESTIC & INTERNATIONAL)

Source: Author's construct, partly adapted from van den Berg (2014:19)

Figure 16: Evolution and development of intelligence, RM and national security

The evolution of these phenomena was only influenced by those in power and the political system applied in a country or region. Therefore, the SA context will be further analysed to determine how SA's framework compares with the conceptualised framework of Chapter Three.

4.3 The Evolution of Intelligence, Risk Management and National Security in South Africa: 1990 to 2022

The SA context needs to be evaluated over the period applicable for the new democratic depensation to determine if SA comply with the necessary principles for an IRM.

4.3.1 The developments of the National Intelligence Framework 1990 to 1996

The SA landscape and political watershed changes from 1990 to 1994 can be described as never-before-seen in world history, with SA changing through a negotiated democracy after apartheid. These developments started in the mid-1980s when the then-Director-General (DG) (Dr Niel Barnard) of the NIS began meetings between the imprisoned Nelson Mandela and the leaders of the ANC in Europe. These meetings influenced SA's intelligence environment and structure – based on democratic principles and standards. These newly-formed intelligence structures were influenced within the context of the negotiated (O'Brien, 2011:208-215) *constitutional and political dispensation*. This historical period has been summarised in the table below, showing which aspects influenced these new intelligence structures and ensured better control, oversight, and legal principles for the military, police, and civilian intelligence services.

Table 8: Historical timeline for the democratic order in SA

Date	Events
2 February 1990	President de Klerk announces that all major political organisations (e.g. ANC, PAC, and CP) are legal and part of the political spectrum.
2 May 1990	The government of SA and the ANC signed the *Groote Schuur Minute*, committing them to a negotiated political settlement.
6 August 1990	The ANC and the government of SA sign the *Pretoria Minute*. Through this agreement, the ANC suspended the armed struggle, and the government released all political prisoners by 30 April 1991; all exiles of political organisations returned to SA to form part of talks about a future constitutional dispensation.
December 1991	All major political parties and organisations supporting a negotiated political settlement meet through the Convention for a Democratic South Africa (CODESA). All organisations sign a declaration of intent, pledging commitment to an inclusive process, which will create a democratically elected constitution-making body.
December 1992	All major parties reconvene at CODESA.
October 1993	Parliament passed the Transitional Executive Council (TEC) Act (Act 151 of 1993) to facilitate the participation of all designated parties (including the liberation movements) in the democratic transition.
26-27 April 1994	SA's first-ever democratic elections are held.
1993-1994	The sub-council on the intelligence of the TEC was formed (in 1993). The sub-council fulfilled a vital role to ensure the agreements on the future intelligence structures, scope and focus. These aspects pave the way for formal structures which comply with the White Paper.
21 October 1994	These changes to the IC in SA were first acknowledged when Minister of Justice Dullah Omar announced the intended new structure of SA's secret services. This was in conjunction with the release of a Government White Paper the same month outlining future policy considerations and

Date	Events
	was followed in December 1994 by three new Acts: The Intelligence Services, The National Strategic Intelligence and The Committee of Members of Parliament and Inspectors-General of Intelligence Acts.
May 1994	Mr Mandela, the country's first president under democratic rule, is sworn into office and his appointed executive deputy vice president, Mr F. W. de Klerk.
June 1996	Under the first democratically elected Parliament's aegis, the Republic of SA's new Constitution (Act 103 of 1996) is adopted.
10 May 1996	The most important of these initiatives was a memorandum of understanding concluded between the South African Police Service (SAPS), the NIA, South African Secret Service (SASS), and the South African National Defence Force (SANDF) which was aimed to ensure the sharing of information relating to combating organised crime.

Source: Author's construct; data adapted from O'Brien (2011:212) and Africa (2009)

Furthermore, the civilian intelligence subcommittee formed under CODESA and the TEC came to some agreements regarding intelligence structures, functions, and reporting lines. They created a new structure and some standards for intelligence services, as shown in Figure 17 below. The organisational design of the intelligence and security environment of SA in 1996 clearly shows that it was explicitly designed with several aspects of good democratic governance in mind, namely executive-level control and oversight, coordination control, and departmental responsibilities. This design also determined the communication lines, responsibilities, and inter-relationships between the different entities/agencies. There are precise executive control and powers, oversight from the ANC structures and government, coordination and communication lines regarding intelligence, and concrete departmental structures with specialised fields of responsibilities. These structures and controlling aspects of intelligence in the newly formed SA context reflect the democratic principles followed by the other democracies (UK, Canada, and Australia, specifically) (O'Brien, 2011:270).

Two types of agreements were of particular relevance during the political negotiations, namely those reached bilaterally between the then-government and the ANC between 1990 and 1992 and those made during the main multilateral decision-making processes in 1991 and 1994. The bilateral and multilateral processes had significant implications for the reform of the security sector and, at each stage, sowed the seeds of new terms of engagement, principles, and rules by which security actors would have to abide.

The organisational design of the intelligence and security environment of SA in 1996, as seen below in Figure 17, clearly shows that it was explicitly designed with good democratic governance aspects in mind. Therefore, all analysts, journalists, commissions, and previous members of these agencies are perturbed by the deterioration and reported failures of civilian intelligence agencies over the past 20 years. The HLRP (2019:2), as appointed by President Ramaphosa in January 2018, attempted to determine *What when wrong*, since the newly designed structures and control measures based on these democratic principles should not have failed and could provide the government with the

necessary national security intelligence. Interestingly, these structures complied well with the conceptualised IRMF proposed in Chapter Three of this dissertation.

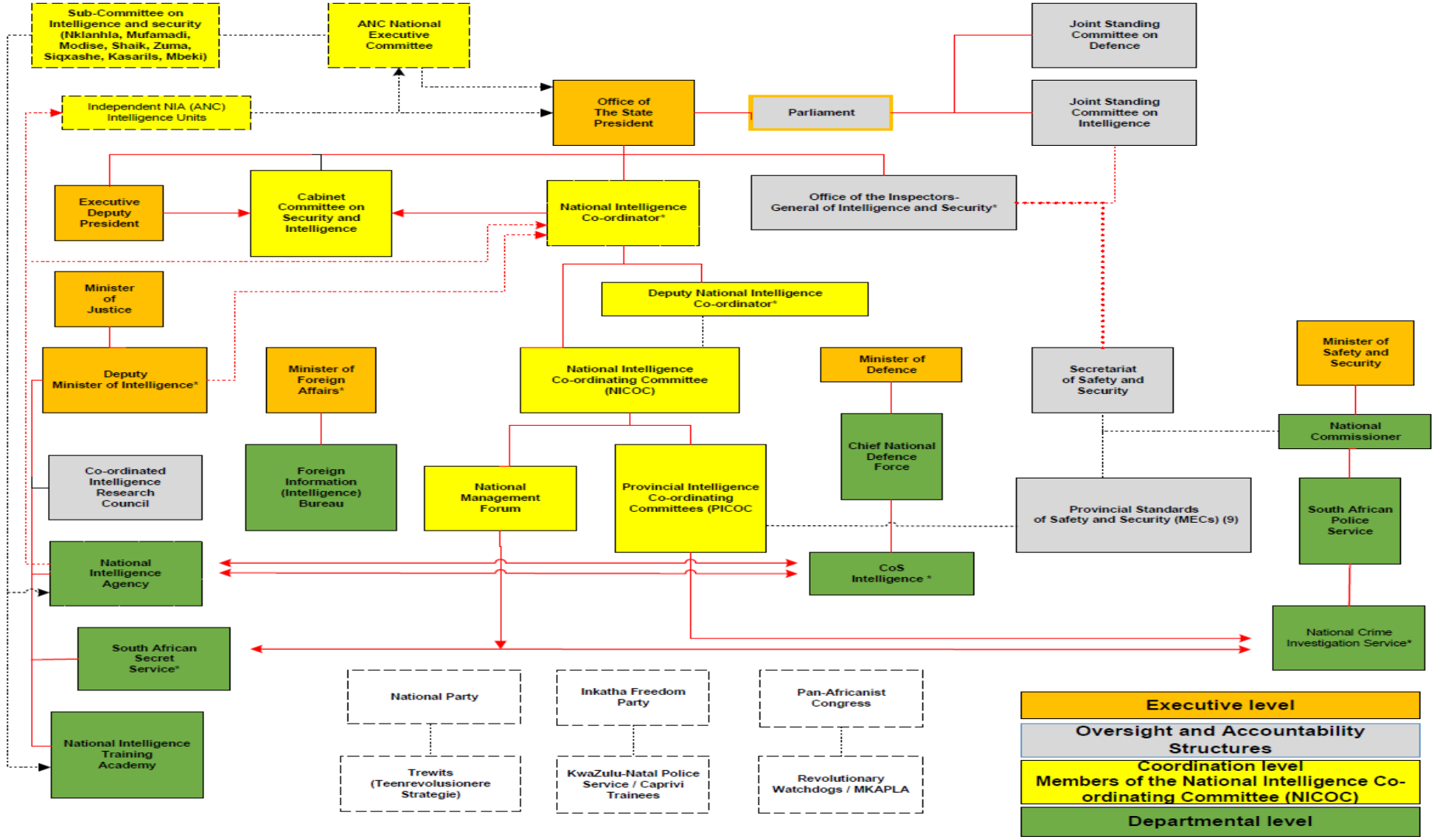
The structures for intelligence (Figure 17) were established by the then-Government of National Unity (GNU) in 1994-95. They lay the foundation for democratic intelligence control and oversight as one of their priorities to ensure reform within the IC. The GNU implemented these aspects because there was no section prescribing intelligence services or functions in the interim 1993 Constitution. After the GNU took office in May 1994, the first step to reform the IC was to publish the White Paper on 2 October 1994. The White Paper on Intelligence outlined the *philosophy, mission, mandates and role of intelligence in SA*. The White Paper (1994:2) also established the following responsibilities for the intelligence and security services:

- *The safeguarding of the Constitution;*
- *the upholding of the individual rights enunciated in the chapter on Fundamental Rights (the Bill of Rights) contained in the Constitution;*
- *the promotion of the inter-related elements of security, stability, cooperation, and development, both within SA and concerning Southern Africa;*
- *the achievement of national prosperity whilst making an active contribution to global peace and other globally defined priorities for the well-being of humankind; and*
- *the promotion of* ***SA's ability to face foreign threats and to enhance its competitiveness in a dynamic world*** [own emphasis].

These aspects align the intelligence structures to comply with a properly defined IRMF and focus their work on providing the necessary IRM for the policy-makers to make informed decisions. Furthermore, the GNU passed legislation in late 1994 which included most of the legalisation control and regulating aspects for the intelligence structures in SA. The listed legislation, which can be viewed as the principal legal mandates for the new intelligence agencies in SA, include:

- *The Committee of Parliament and Inspectors-General of Intelligence Act (40 of 1994) created intelligence oversight mechanisms*.
- *The Intelligence Services Act (38 of 1994) created the civilian National Intelligence Agency (NIA) and the SASS.*
- *The National Strategic Intelligence Act (39 of 1994) defined the functions of the NIA, and SASS, and created a National Intelligence Coordinating Committee.*

This legislative framework was amended throughout the next 20 years and should impact the IC's processes and products. However, as reported by commissions, review panels, task teams, and media reports, it did not create the necessary change to influence intelligence products at executive levels of government. Below is a detailed analysis of these Acts compared to the IRMF.



Source: Adapted from O'Brien (2011:213)

Figure 17: The SA intelligence and security structures - 1996

4.3.2 A comparative analysis of the legal framework, structures, and incidences of failure for intelligence in SA from 1996 to 2021

This section will analyse the legal frameworks, structures, and incidences from an IRMF perspective to determine if an IRMF framework can be implemented in SA. The first focus will be the intelligence framework, secondly the RM field, and lastly, the national security environment.

4.3.2.1 The intelligence framework of South Africa from a legal perspective

SA's intelligence framework from 1996 to 2021, even with its changes, is divided between executive, coordination, and departmental levels with particular communication and control lines for these intelligence and security services. The structures from 2003 (Figure 18) show that democratic principles were followed in the design of these different levels, in line with the legislation framework. Figure 18 also shows the executive political command and control, communication lines, oversight, coordination, and departmental levels in the intelligence environment until 2010.

4.3.2.2 Executive and governance level: President, Parliament, ministerial and oversight

Chapter 11 of the Constitution describes the legal standing of the intelligence and security services and frameworks. The Constitution was drafted with democratic principles and control as its guiding foundation. Sub-section 198 (a-d) states which legal principles must be complied with by all security services to serve the republic and all the country's people:

(a) National security must reflect the resolve of SA, as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want, and to seek a better life.

(b) The resolve to live in peace and harmony precludes any SA citizen from participating in armed conflict, nationally or internationally, except as provided for in terms of the Constitution or national legislation.

(c) National security must be pursued in compliance with the law, including international law.

(d) National security is subject to the authority of Parliament and the national executive.

These principles direct intelligence and security services to comply with particular ethics, norms, and professionalism. They must respect other people's rights and adhere to the rule of law (domestically and internationally) and Parliament, as well as the executives authorising their work. (White Paper 1994). Furthermore, sub-section 199 of the Constitution establishes, structures and directs the conduct of security services and declares that structures will be approved by Parliament, and legislation should determine their establishment, structures and work:

(1) The Republic's security services consist of a single defence force, a single police service, and any intelligence services established in terms of the Constitution.

(2) The defence force is the only lawful military force in the Republic.

(3) Other than the security services established in the Constitution, armed organisations or services may be established only in terms of national legislation.

(4) The security services must be structured and regulated by national legislation.

(5) The security services must act and teach and require their members to act, following the Constitution and the law, including customary international law and international agreements binding on the Republic.

(6) No member of any security service may obey a manifestly illegal order.

(7) Neither the security services nor any of their members, may, in the performance of their functions-

(a) prejudice a political party interest that is legitimate in terms of the Constitution; or

(h) further in a partisan manner, any interest of a political party

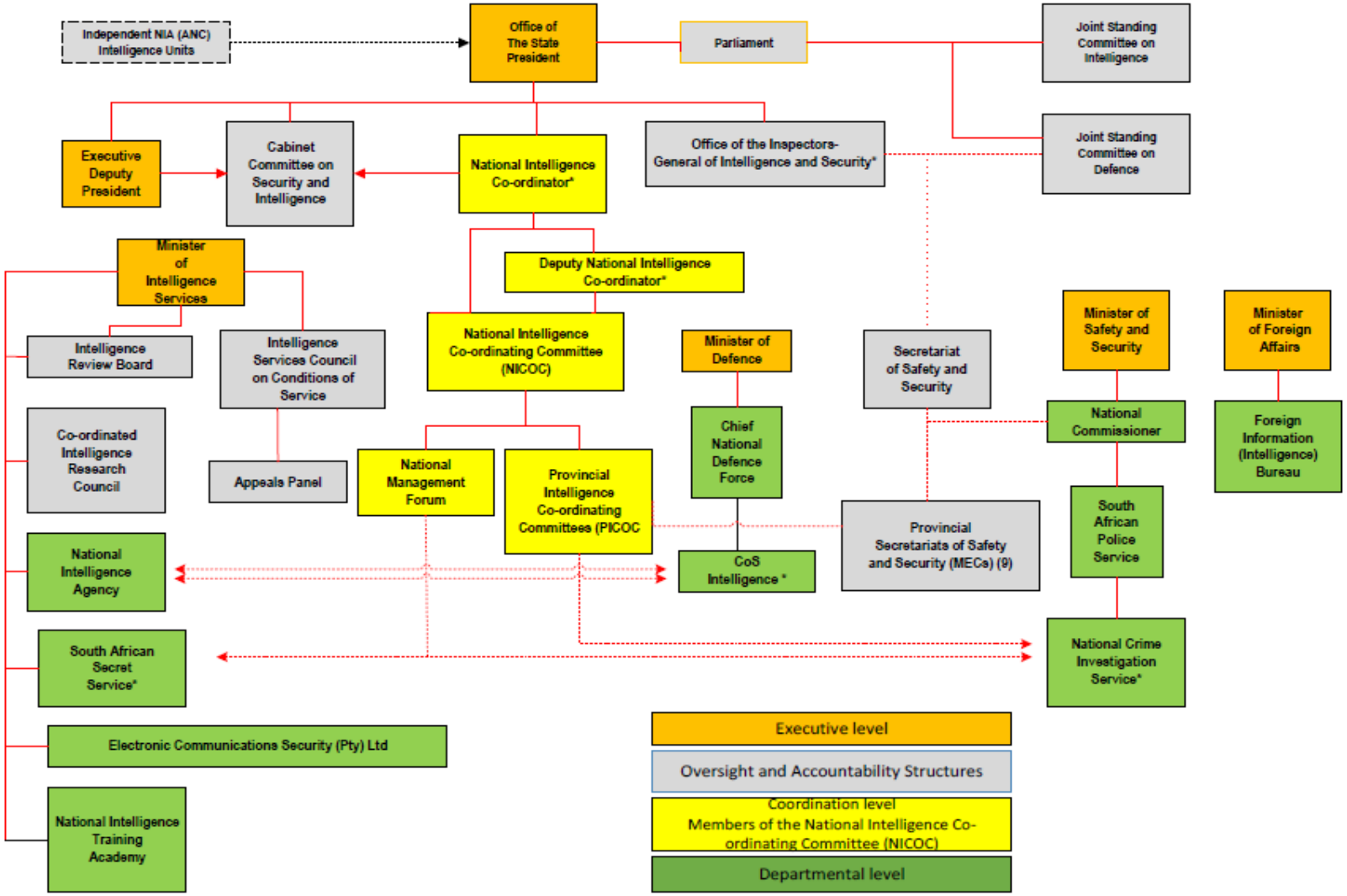
(8) To give effect to the principles of transparency and accountability, multi-party Parliamentary committees must have oversight of all security services in a manner determined by national legislation or the rules and orders of Parliament.

The above rules apply to SA's intelligence and security services. The Constitution further expanded its rules and direction for security and IC in Chapter 11, which becomes more specific for each of these services. Therefore, the focus of this sub-section will be to analyse the IC only. Sub-section 209 spells out the establishment and control of intelligence services, with particular indications for civilian intelligence agencies' rules:

*(1) Any intelligence service, other than any intelligence division of the defence force or police service, may be established only by **the President**, as head of the national executive, and only in terms of national legislation.*

*(2) The President as **head of the national executive must appoint** a woman or a man as head of each intelligence service established in terms of sub-section (1) and must either assume political responsibility for the control and direction of any of those services or designate a member of the Cabinet to assume that responsibility.*

Only the president can approve the above rules and establishment of these structures, which must comply with aspects mentioned in Chapter Three for a conceptualised IRMF. These aspects of the Constitution are also in line with democratic principles for controlling and establishing intelligence agencies in the rest of the world. Sub-section 210 states that these agencies must be controlled by national legislation, which determines their objects, powers, and functions.



Source: Adapted from O'Brien (2011:213)

Figure 18:The intelligence structure of SA (2003)

These rules include any intelligence division of the defence force or police service and must provide for:

(a) The coordination of all intelligence services; and

(b) civilian monitoring of the activities of those services by an inspector appointed by the President, as head of the national executive, and approved by a resolution adopted by the National Assembly with a supporting vote of at least two-thirds of its members.

The above constitutional principles affect several democratic rules for the practice of intelligence services and how they will be controlled, overseen, and governance applied in their environment by the President, ministers, Parliament, Parliamentary committees, and bodies. This sub-section (210) of the Constitution includes one significant paragraph which will ensure that an IRMF can be implemented in the Republic. It provides the necessary balance between secrecy and transparency in the application of intelligence work which provides better communication, control, and understanding of the functions of the IC and policy-makers. Therefore, the Constitution, with one subparagraph (210) summarises this significant oversight and governance of intelligence and security services which should:

(8) …give effect to the principles of transparency and accountability, multi-party Parliamentary committees must have oversight of all security services in a manner determined by national legislation or the rules and orders of Parliament.

In its preamble, the Constitution states that: *the foundation for a democratic and open society in which government is based on the will of the people and every citizen is equally protected by law*. Thus, this statement leaves little room for anyone to disrespect the Constitution as the legal and ethical framework that determines the work of the intelligence and security community as supreme law.

The IC has complied with the Constitution by developing the necessary national legal framework, which determines its structures, mandates, as well as national security threats of focus, functions, and responsibilities. The legislative framework was developed from 1994 to 2002, which included a framework that put the necessary control mechanisms in place. These Acts, policies, and regulations were aligned with the Constitution and are listed below:

- Protection of Information Act No. 82 of 84, Replacement Bill on the table: Protection of State Information *[B6-2010].* The Bill was passed on 29 November 2012 with amendments by the National Council of Provinces. On 25 April 2012, the National Assembly approved it. However, in September 2013, then-President Zuma refused to sign the Bill into law, sending it back to the National Assembly for review;
- Public Finance Management Act No. 1 of 1999;

- Regulation of Interception of Communication and Provision of Communication Related Information Act No. 70 of 2002;
- The Intelligence Services Act No. 65 of 2002;
- The Intelligence Services Oversight Act No. 40 of 1994;
- The National Strategic Intelligence Act No. 39 of 1994;
- The Public Service Act No. 103 of 1994;
- The Public Service Regulations (Issued in 2016).
- The Treasury Regulations as amended (Issued in 2001); and
- The White Paper on Intelligence 1994;

The most significant change in the civilian intelligence legal framework, also identified by the HLRP (2018-19), was during the 2010-2013 period. The change was made through the GILAA. It impacted the name of the civilian intelligence agencies from NIA, SASS, South African National Academy for Intelligence (SANAI), and National Communication (NC) to the State Security Agency (SSA). The GILAA amended the National Strategic Intelligence Act, explicitly defining the national threats on which the services should focus. These changes broadened the scope of the civilian intelligence agency to include anything viewed as a threat, risk, or vulnerability that they must attend to. The original definition in the National Strategic Intelligence Act (39/1994: s 1) states that the intelligence agencies must focus on *counterintelligence measures and activities conducted, instituted or taken to impede and to neutralise the effectiveness of foreign or hostile intelligence operations, to protect intelligence and any classified information, to conduct [security screening] vetting investigations and to counter [subversion, treason, sabotage, and terrorism aimed at or against personnel, strategic installation or resources of the Republic].*

The GILAA (2013) amended the Act to read: *any threat or potential threat to national security*. The definition gives the agency a vast threat target field to counter anything that it views as a threat. These aspects will be discussed later in the sub-section on national security. These aspects also influence the civilian intelligence environment's structuring, policies, and regulations. The incidences regarding the particular Special Operations Unit (SO) and its activities come to mind. They disregard the professional conduct of intelligence officers as prescribed by the Constitution. Furthermore, the unit focuses on all threats and risks as the agency sees fit. These actions disregard the proper understanding of the laws applicable to these types of operations. The HLRP (2019:55) states that *the SSA Special Operations (SO) unit in terms of its serious breaches of the Constitution, legislation, and other prescripts, mainly related to the politicisation and factionalisation of intelligence as well executive overreach. It just needs to be noted here that the SO became a law unto itself, particularly in terms of utilising and accounting for SSA funds, and its very existence and functioning was a prime example of the devastating impact.*

The unit's actions directly breach the Constitution, the White Paper, the relevant legislation, and good government intelligence functioning. These aspects could be controlled and corrected by ministers or the president with broad political powers, as analysed below.

A **president**, as the head of the national executive, has the power to create structures, appoint people in the civilian IC, dismiss appointed executives and request reports regarding national security issues. From an intelligence perspective, the Presidential powers and oversight are given through the legal framework, as summarised in the table below. Furthermore, the Constitution's sub-section 101 determines that the President must make these executive decisions by following these rules:

(1) A decision by the President must be in writing if it-

(a) is taken in terms of legislation; or

(b) has legal consequences.

(2) A written decision must be counter-signed by another Cabinet member if that decision concerns a function assigned to that other Cabinet member.

(3) Proclamations, regulations, and other instruments of subordinate legislation must be accessible to the public.

(4) National legislation may specify how and the extent to which instruments mentioned in sub-section (3) must be-

(a) tabled in Parliament; and

(b) approved by Parliament.

Table 9: Legal framework of the President's powers and oversight from an intelligence perspective

Acts	Sections	Powers and oversight
Constitution 1996	Section 91 (2)	*To appoint Ministers and Deputy Ministers assigns their powers and functions and may dismiss them.*
	Section 197 (4)	*To appoint on the recommendation of the National Assembly, the Public Protector, the Auditor-General (AG) and the members of other constitutional commissions.*
	Section 209 (1)	*Which governs the establishment of civilian intelligence services,*
	Section 209 (2)	*Must appoint a woman or a man as head of each intelligence service established.*
	Section 210 (b)	*To appoint an Inspector-General (IG) who is approved by a resolution adopted by the National Assembly with a supporting vote of at least two-thirds of its members.*
Intelligence Services Act, No. 65 of 2002	Chapter II, section 3(3)(a)	*State that: the President must appoint a DG for each of the Intelligence Services.*
	Chapter II, section 4 (2)	*State that: the creation of Deputy Directors-General posts by the Minister must be done in consultation with the President.*
	Chapter II, section 6 (1)	*State that: The President must follow the Public Service Act, 1994 (Proclamation 103 of 1994), appoint ahead of the Academy who is also the Chief Executive Officer, principal, and accounting officer of the Academy. These appointments have changed due to the amalgamation of all the structures into the SSA (2013).*
Intelligence Services Oversight Act, No. 40 of 1994	Section 2 (3) (a)	State that a member of the Joint Standing Committee on Intelligence (JSCI) shall be appointed by the Speaker or the Chairperson of the National Council of Provinces, depending upon the House of Parliament from which the member is appointed, acting with the ***concurrence*** of the President, who shall act with the concurrence of the leader of the political party concerned.

Acts	Sections	Powers and oversight
	Section 2 (3) *(b)*	*State that: If an agreement is not reached in respect of the appointment of a particular member, **in the JSCI**, the matter shall be referred for determination to a committee consisting of the President, the Speaker, the Chairperson of the National Council of Provinces and the leader of the political party concerned, and the decision of the committee shall be final.*
	Section 2 (3) (b)	State that: *The Speaker and the Chairperson of the National Council of Provinces acting with the concurrence of the President, who shall act after consultation with the leaders of the political parties represented on the Committee, shall appoint a member of Parliament, excluding a member appointed to the Committee in terms of sub-section (3), as the chairperson of the Committee.*
	Section 7 (1) (a-b)	State that: *the President shall appoint an IG of Intelligence- (a) nominated by the Committee (JSCI), and (b) approved by the National Assembly by a resolution supported by at least two-thirds of its members.*
	Section 7 (3 -5)	State that the President determines the remuneration and other employment conditions, removes or suspends the IG and tasks, and receives IG reports.
National Strategic Intelligence Act, No. 39 of 1994	Section 7 (1)	State that: *the President shall appoint a person as Co-ordinator for Intelligence, who shall, subject to the directions and supervision of the Minister- (a) manage and administer the functions of National Intelligence Co-ordinating Committee (NICOC).*
The White Paper on Intelligence	Paragraph 6.2	State that: *A Coordinator will chair NICOC for Intelligence (Appointed by the President) who will be accountable to the President.*

Source: Author's construct

The above-described powers and authority of the President can be highlighted by five incidents that occurred over the past 20 years in SA. Africa and Mlombile (2001:8-9) state that a senior executive of the military informed President Mandela's administration that some of the ANC elite were planning to undermine the negotiation process; later, in the 1990s, executives of the SANDF were 'plotting a coup'. These reports were found to be false and were dismissed by investigation and evaluation task teams. These reports reached the Presidency directly, not through the approved and verified channels (NICOC); thus, the senior member was replaced and left the service soon after.

The second incident of interest was then-President Mbeki's dismissal of the DG NIA in 2005. This decision was questioned in court by Mr Masetlha (Masetlha v President of RSA and Another, 2008 [1] SA 566 [CC]). The courts ruled that the President acted inside his powers to dismiss the DG, notwithstanding that Masetlha was exempted from all wrongdoing when he conducted a specific surveillance operation. The way this incident was handled proves that the SA intelligence framework does work under the democratic principles described in the Constitution, White Paper, and other intelligence legalisation.

A third scandal arose from the *Browse Mole Report* (Africa and Mlombile, 2001:8-9), prepared by the Directorate of Special Operations (DSO) or 'Scorpions', as it was popularly known. Although not an intelligence agency, the DSO led an operation using intrusive intelligence methods, which led it to claim that certain African governments - including those of Libya and Angola - were funding a conspiracy by the Deputy President of the ANC, Zuma. The president and cabinet approved that the government disband the DSO. Pauw (2017:36-39) states that *during Fraser's investigation into the*

Browse Mole report, the NIA tapped the phones of several high-ranking officials mentioned in the report, including those of Ngcuka and Leonard McCarthy, the Scorpions boss. On the tapes, they discussed when would be the most politically damaging time to charge Zuma. Fraser had unearthed what amounted to gold for Zuma. Notwithstanding the official inquiries, the ruling party (ANC) investigated the e-mail saga. *This blurring of the lines between state and party business left many SA confused and suspicious that state institutions served at the behest of the ruling party* (Africa and Mlombile, 2001:8-9). Pauw (2017) indicates that somebody was covering up for Zuma and that the intelligence structures under Fraser can easily be those who were protecting him. Therefore, intelligence was misused by political leaders for their political agendas and work.

Regardless, the above clearly shows that SA's legislative framework gives the President the necessary critical powers and control aspects regarding the intelligence environment. Furthermore, this aligns the intelligence framework with the conceptualised IRMF of Chapter Three.

Furthermore, the above rules of the Constitution also provide **Parliament's** control and authority regarding security services. These rules provide essential aspects of the intelligence environment, namely planning, budgeting, work ethics, and norms. The Constitution, section 44 (1)(a)(ii) states that *the national legislative authority as vested in Parliament- (a) confers on the National Assembly the power- (i) to amend the Constitution; and (ii) to pass legislation concerning any matter, including a matter within a functional area listed in Schedule 4.*

Therefore, all intelligence legislation is approved by Parliament and is binding on these structures. All these structures must provide feedback to Parliament every year regarding their strategies, spending, activities, risk experience, successes, and problems during the past year. The intelligence environment feedback occurs through different forums in Parliament, such as different ministers' budget speeches and feedback, the JSCI, AG and Parliamentary oversight structures. Over the years, Parliament was briefed on successes but more about intelligence failures. The NIA provided information to Parliament during 2001-2004 regarding the successful counter actions of the threats of violence (PAGAD), specifically in the Western Cape. The actions of the NIA led to the arrest and prosecution of several people involved. Furthermore, the NIA plays an essential role in collecting intelligence regarding violence in the taxi industry. Africa (2011:24) mentioned that the NIA was also involved in joint operations with SAPS to combat internal stability issues and organised crime.

Notwithstanding these successes, the NIA was faced with embarrassment and negative media reports regarding counterintelligence operations. After these operational failures in 2004-2005, the minister of intelligence took action against several senior management members, including the DG NIA. This situation led to court cases between these members, the President, the minister, and NIA (Masetlha,

2005). These cases show that members do not follow or comply with the rules and prescripts of the Constitution and the White Paper; however, in the end, members were acquitted of any wrongdoing.

The above shows that the President and Parliament have authority and control of overseeing the intelligence services' planning, budgeting, functions, and activities. They are supported with these political and administrative functions by the responsible ministers and deputy ministers appointed in these areas. The responsibilities of these ministries will now be further analysed.

The **minister and deputy minister** responsible for intelligence services are appointed by the President in terms of section 209(2) of the Constitution. They must exercise political responsibility, administrative governance, and oversight for the control and direction of the civilian intelligence services. These offices are supported by ministerial staff. The minister or/and deputy minister responsible for the environment must implement a policy framework that defines and controls the services' activities. These ministries must further ensure that services comply with these arrangements and, if not, initiate a commission, task team or investigation of whether the services comply with legislation, regulations, policies or directives. The minister activated such a commission after the 2005 scandals (Masetlha v President of the RSA and Another, 2008 [1] SA 566 [CC] para 33). These aspects harm the image of civilian intelligence agencies. Thus, according to Africa (2011:24), Minister Lindiwe Sisulu went on a public relations drive to improve the agencies' image with the public, media, and universities in SA. The minister's actions furthered the development of intelligence websites, which give a more transparent picture of the IC, thereby broadening a balance between secrecy and transparency in the work of intelligence services in SA.

Furthermore, the public relations drive created a way to open some aspects of intelligence up to the general public and help to reflect a better image of the secret world of espionage. These websites contained information regarding the mission, vision, organisational values, and what intelligence entails, as well as the structuring of departments and branches, their responsibilities and targets, basic intelligence processes and products, and which tasks are directed to these departments and branches. The sites also delved into indicators of deliberate intent to cause potential harm to the state or its citizens, the oversight of intelligence, and what threats to national security they focus on. Over the years, these websites also contained structures and graphics regarding the intelligence environment. Intelligence services are also required to justify interceptions (for example, electronic communications, surveillance, and some intrusive methods) as a method of investigation or collection (BusinessTech, 2021). A Judge is appointed to oversee these activities, and the services must apply with motivation. Therefore, ministers must ensure that the necessary policies, regulations, or directives that control these aspects are in place. However, the incidents around the NIA mentioned above point to several gaps in regulatory control. These were also confirmed by a ministerial review commission (2008) and

the HLRP (2019) (created by the serving minister for intelligence and the President). Pauw (2017) mentions the spy tapes regarding former President Zuma which play an important part in the weapon transaction case. These reviews found inadequate controls over the intelligence services' clandestine operations. The JSCI report (2020) also captured in an annexure the Judge for approval of the interception report that services and individual members are not complying with the legal applications for these activities.

Moreover, the above information from the judge questioned the ethics, norms, and professionalism of services and members of the senior executive level of the different departments in the IC of SA. These observations were meant to remind SA of the possible harm intelligence services can cause if they are not properly regulated and that ministers and deputy ministers need to take serious action to correct these misconducts. These incidents show that from the political executive levels to the operational levels in departments, the human factor is a threat to the intelligence framework in SA. Equally, the HLRP (2019:2) states that all these aspects create a human environment where members, frameworks and work of the IC are:

- ***Politicisation****: The growing contagion of the civilian IC by the factionalism in the ANC progressively worsened from 2009.*
- ***Doctrinal shift****: From about 2009, there was a marked doctrinal shift in the IC away from the prescripts of the Constitution, the White Paper, and the human security philosophy towards a much narrower, state security orientation.*
- ***Amalgamation****: The amalgamation of the NIA and the SASS into the SSA did not achieve its purported objectives and was contrary to existing policy.*
- ***Secrecy****: A disproportionate application of secrecy in the SSA stifles effective accountability.*
- ***Resource abuse****: The SSA had become a 'cash cow' for many inside and outside the Agency.*

An intelligence environment as described above will not be conducive to an IRMF. These poor results at the executive level influence the IC at the oversight, coordination, and departmental levels. These levels will be analysed further below.

The observations above, as made by the HLRP, also reflected on the **oversight organisations** for intelligence. These state organs will be analysed and compared with democratic principles below.

During former President Mbeki's first administration (2000), a **National Security Council** was established to provide high-level intelligence and security advice, as well as coordinate all security sector activities. The council was a non-statutory body created by a cabinet decision in 2000. Therefore, SA's NSC is the high-level inter-ministerial council; it includes senior ministers and officials and aims to deal with a wide range of threats to national security and stability – whether malicious or

naturally-occurring. However, members meet irregularly to deal with specific crises rather than following the normal processes of government. From all appearances, decision-making on national security issues – as with several other leading policy issues – resides within the Office of the President rather than in the NSC or other more consultative fora. According to the HLRP (2019), this committee attended to *acting at a strategic level – and overseeing bodies and programmes such as the National Disaster Management System and the Cabinet Committee on Security and Intelligence (CCSI) would support SA-led activities domestically and throughout sub-Saharan Africa*.

However, the council activities have stopped for reasons unknown. The HLRP (2019) states that the NSC, which last sat during former President Mbeki's administration, must urgently be re-established to provide the necessary coordination and oversight function to the intelligence and security services. In his budget speech for 2020, the President indicated that the council would be re-established. According to a notice in the Government Gazette, Proclamation No. 13 of 2020, the President, who will also chair the NSC, signed the proclamation on February 27 to re-establish this significant council for intelligence and security.

The principle of making intelligence accountable to Parliament is a high point in the democratic evolution of SA. However, its practical implementation depends on the vigilance of the concerned Parliamentarians. The **Joint Standing Committee on Intelligence** (JSCI) comprises members of Parliament nominated through a prescribed proportional formula of members of Parliamentary political parties. The JSCI oversees the intelligence and counterintelligence functions of the intelligence structures, their administration, financial management, and the agencies' expenditure. The Intelligence Services Oversight Act No. 40 of 1994 (specifically sections 2–3), describes the establishment and responsibilities of the JSCI, which include:

- Governance and control over the foreign and domestic functions of the civilian intelligence services;
- Financial and administrative reports received from the Minister of State Security and the IG for intelligence;
- Make recommendations on intelligence-related legislation and regulations; and
- Give feedback to Parliament regarding the status of the work of these intelligence services.

The JSCI is empowered by the above-Act to fulfil, *among other things,* the following functions:

- To obtain an audit report of the intelligence services from the AG;
- To obtain a report regarding the functions performed by the judge designated to authorise intrusive methods of investigation;
- To review and make recommendations regarding interdepartmental cooperation and the rationalisation and demarcation of functions;
- To order investigations into complaints from the public; and

- To hold hearings and subpoena witnesses on matters relating to intelligence.

Concerning financial and judicial oversight, the JSCI cooperates with the Offices of the AG and the specially appointed judge for electronic interception. These offices will ensure that proper auditing, approvals and control are conducted in the intelligence environment regarding these aspects.

The JSCI has also encountered numerous problems in politicisation and concerns over the integrity of the Committee's members of various political parties (Africa, 2011). The JSCI identified several incidents of misconduct in the IC. In the *Browse Mole Report* saga, the NIA investigations into the source of the claims led them to the DSO (or Scorpions) investigators (Africa, 2011). When receiving a report on the NIA investigation, the JSCI condemned the DSO, claiming its reckless reporting had jeopardised national security. Moreover, they questioned why the DSO was engaged in intelligence activity outside its legal mandate whilst using intrusive intelligence methods. Given the subject matter of the *Report*, it appeared that yet another security organ had been caught up in political conflict.

In addition, the Committee's 2021 report (which missed its deadline, as it has done many times before), indicated problems experienced due to Covid-19 lockdown phases in SA (HLRP, 2018:96). The JSCI (2021) report confirmed most aspects reported to the Zondo Commission by the Acting DG of the SSA. Part of the JSCI's report (AG report), indicated that they had difficulty correctly auditing the covert/special operation environment of the SSA. The judge's report on the IC's electronic interception cases showed that both services and members were misusing the system to obtain approval for interceptions by i) making false statements and ii) hiding figures (BusinessTech, 2021). The Constitutional Court ruling on interception under the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) confirms that the IC must improve its work regarding these aspects of intelligence work. The Court ruled that people's right to have their information intercepted was not adequately verified in the Act, thus **it** must be refined to ensure these aspects are appropriately applied (BusinessTech, 2021).

The JSCI (2021) report shows that the members serving in the intelligence environment seriously threaten good governance, management, administration and operational practices. These aspects will hamper the implementation of an IRMF in the SA intelligence environment. An IRMF needs all these aspects to be applied at an outstanding level to function correctly. These human beings in the system, which are working to reach their agendas, will block the implementation of IRMF because it will identify all their wrongdoing during the project planning, and action will be taken against them.

Section 210 of the Constitution and the Intelligence Services Oversight Act, specifically section 7(1), approved that the President may appoint an ***Inspector General for Intelligence*** after being nominated by the JSCI and approved by Parliament. The IG is authorised with vast oversight powers and access to the intelligence environment to investigate any aspects of its work. The Office of the Inspector-General of Intelligence (OIGI) monitors the Intelligence Services. According to the Act section 7, the functions of the IG are:

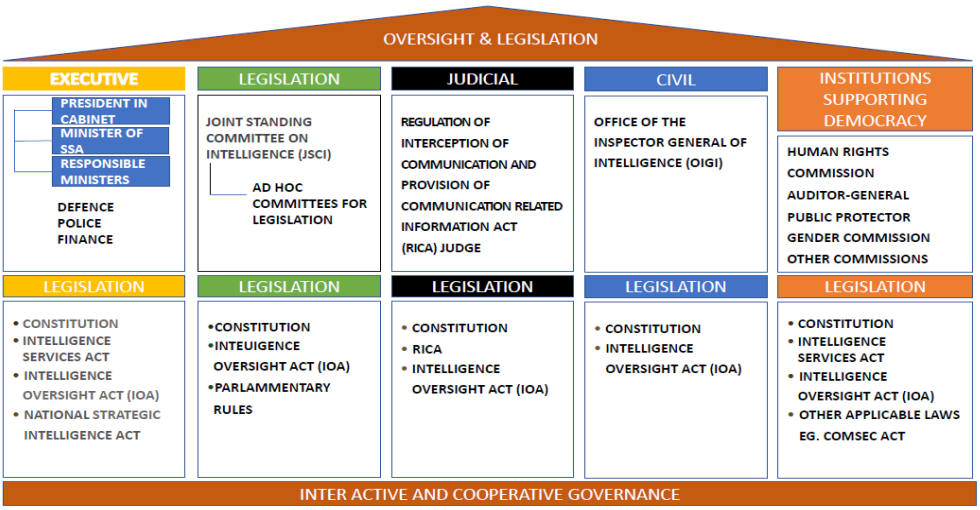
- *to monitor compliance by any Service with the Constitution, applicable laws and relevant policies on intelligence and counter-intelligence;*
- *to review the intelligence and counter-intelligence activities of any Service;*
- *to perform all functions designated to him or her by the President or any Minister responsible for a Service;*
- *to receive and investigate complaints from members of the public and members of the Services on alleged maladministration, abuse of power, transgressions of the Constitution, laws and policies*.

The IG will report to the JSCI for their office's overall function and provide feedback on all-year reports and new legislative proposals (BusinessTech, 2021). The intelligence oversight portfolio has perhaps seen some of the most significant problems encountered in establishing transparent and independent intelligence functions within the post-apartheid government (News24, 2021), including an inability to permanently fill the IG's post for almost the first decade of the new dispensation (HLRP, 2018:93-95). In addition, the IG was drawn into investigating claims surrounding a related hoax e-mail (Masethla and others) scandal emanating from the NIA (Africa, 2011:24). The IG office was also a critical player in criminal investigations that transpired against senior officials of the NIA. Among the charges laid was the failure to disclose information to the IG as provided for in the Intelligence Services Oversight Act. Another fraud charge related to the falsification of intelligence provided to the President. These long-drawn-out cases tested the capacity of the IG and state and it became evident that the intrigue related to a power struggle within the ruling party (ANC). In the end, the charges were either withdrawn or the accused acquitted. Importantly, the IG office's existence proved to be an essential oversight instrument (Masetlha v President of the RSA and Another, 2008 [1] SA 566 [CC] para 33).

The **Auditor General** provides additional financial oversight on all funds spent by the civilian intelligence services. All the intelligence and security services functions (including intelligence, although with some limitations) are subject to routine government auditing procedures and scrutiny by the Parliamentary Standing Committee on Public Accounts (SCOPA). The HLRP (2019:53) states that the *Ministry and agency should urgently find with the AG an acceptable method for the unfettered auditing of the agency's finances, including covert finances that leads to the absence of the standard qualification in the Agency's annual audits* because, unfortunately, the special operational unit

committed several financial errors and tried to cover-up maladministration through false documentation.

In addition, the IC are subject to **oversight by human rights monitoring agencies**, such as the Public Protector; SAHRC; Commission for the Promotion and Protection of the Rights of Cultural, Religious and Linguistic Communities (CRL Rights Commission), and the Commission for Gender Equality (CGE), as an ongoing reflection of SA's close involvement of civilian bodies in its development. Anyone can file a complaint with these commissions involving the IC. Figure 19 below reflects all the intelligence oversight structures in SA. These commissions also link up to the coordination level.



Source: Reconstructed from State Security Agency Ministerial website (2020)

Figure 19:Several bodies provide oversight of the intelligence services

4.3.2.3 The coordination level:

The **National Intelligence Coordinating Committee** (NICOC) was established in the National Strategic Intelligence Act, No. 66 of 2002 (as amended). NICOC is an interdepartmental intelligence coordinating mechanism and is chaired by a coordinator. NICOC members include the DG SSA, directors of foreign and domestic branches of the SSA, *the chief of the intelligence division of the SANDF, the head of the intelligence division of the SAPS, and members of departments of state whom NICOC co-opts on a permanent or an ad hoc basis* (Act 66 of 2002: s 4). In addition, the White Paper (1995) states that: *NICOC will coordinate the activities of the IC and act as the key link between the IC and policy-makers*. Furthermore, Act No. 66 of 2002, section 4(2) stipulates that NICOC will be responsible:

(a) to coordinate the intelligence supplied by the members of the National Intelligence Structures to NICOC and interpret such intelligence for use by the State and the Cabinet for -

(i) the detection and identification of any threat or potential threat to the national security of the Republic;

(ii) the protection and promotion of the national interests of the Republic;

(b) for the purposes of the functions contemplated in paragraph (a)-

(i) to co-ordinate and prioritise intelligence activities within the National Intelligence Structures;

(ii) to prepare and interpret intelligence estimates;

(c) to produce and disseminate intelligence which may have an influence on any state policy with regard to matters referred to in paragraph (a) for consideration by the Cabinet;

(d) after consultation with the departments of the State entrusted with the maintenance of the security of the Republic, to coordinate the flow of national strategic intelligence between such departments;

(e) at the request of any Department of State, to coordinate the gathering of intelligence and without delay to evaluate and transmit such intelligence and any other intelligence at the disposal of the National Intelligence Structures and which constitutes departmental intelligence, to the department concerned; and (f) to make recommendations to the Cabinet on intelligence priorities.

(3) The Agency shall provide logistical, technical, and administrative support to NICOC.

The above information clearly shows NICOC's role in overseeing the coordination of intelligence activities, analyses, and interpretations of intelligence reports in order to give feedback to the President through the CCSI. Furthermore, NICOC ensures no duplication of functions and collection by the different services. These aspects ensure that cost-effective intelligence products are compiled. As mentioned previously (Africa & Kwadjo, 2001), the Chief of Defence Intelligence (DI) hand-delivered a sensitive report to President Mandela claiming that senior members of the SANDF plotted a coup. This document did not follow the correct communication channels, was not verified, and contained incorrect information. The member was relieved from his position. The incident shows that NICOC, as a coordinating body, does have a crucial role in the IC of SA. SA is not the only country to face coordination issues; Walsh (2011:55) mentions that after Australia's Hendra virus outbreak, the country learnt that a speedy response was hampered by poor coordination and ill-involved role-players. That said, the intelligence coordination functions in SA compare well with international standards. Therefore, the coordination of intelligence can ensure that an IRMF can, with minor adjustments, be implemented in SA.

The HLRP's (2019:3) report states that not everything is applied according to the above-indicated functions of the NICOC or according to their dedicated responsibilities to the IC and the country's leaders. The report further recommends that NICOC report to the Presidency and that all IC mandates/structures be better defined to ensure coordination. Thus, departmental-level mandates and functions will play a vital role in adequately coordinating intelligence, as analysed below.

4.3.2.4 Departmental level

SA has undergone a profound transformation and changes in its intelligence and security sectors after 1994. These reforms involved integrating apartheid-era intelligence, military, and police services with those of the liberation movements. These services had to comply with the new democratically formulated legislation and principles. Thus, the founders of the new Constitutional order ensured that these services were controlled by the Constitution, Acts and policy guidelines for a democratic state.

Amalgamation and rationalisation occurred in the intelligence establishment, and two separate services were created between domestic (NIA) and foreign (SASS) intelligence concerns in 1996 (see Figure 18 above). In 2010, these two services were merged into the SSA, which created unnecessary problems and disagreements. The analyses show that serious problems are still experienced, including factionalism, politicisation, and corruption. Until the IC can function as a professional, ethical, and well-trained department(s), suspicions regarding its function will continue.

Considering the above background, analysing the Intelligence Services Act No. 65 of 2002 legally binds the establishment, composition, administration, and control of the civilian intelligence environment. The Act explicitly provides for the accountabilities and responsibilities of the heads of these services; specifies the responsibilities and duties of the members; stipulates composition, administration and regulations of the Intelligence Services Council on Conditions of Service; and provides for general political governance and control of the Minister for State Security.

Notably, the White Paper, which was the foundation from which these legislations were formulated, reflects the vision and values of the founders of our constitutional democracy as far as democratic intelligence is concerned. The White Paper (1994) sets out the legislative mandate of the new civilian services (domestic and foreign) and aims to address the creation of an effective, integrated, and responsive intelligence machinery that can serve the Constitution and the government of the day through the timeous provision of relevant, credible, and reliable intelligence. Therefore, the White Paper (1994) and the ministerial website describes modern intelligence as:

- *Organised policy-related information,*
- *including secret information 'that may be gathered by covert or overt means,*
- *from a range of sources, human and non-human, open or secret*.

In addition, it recognises various forms of intelligence, including political, economic, technological, scientific, military, criminal, and counterintelligence. SA's IC is well structured, directed and focused, and compares well with counterparts in the rest of the democratic world. These aspects lean towards the successful implementation of an IRMF in their environment, which will provide the necessary

managerial tools to overcome problems experienced in their environment. The core outcomes of an IRMF provide the necessary strategic intelligence for threats, risks, vulnerabilities, and opportunities.

According to the White Paper (1994) and the SSA ministerial website,(2020) for intelligence to remain relevant in the modern, post-Cold War world, intelligence must serve the following purposes from an IRMF perspective (White Paper, 1994:3):

- *Provide policy-makers timeous, critical and unique information to warn them of **potential threats**, **risks**, **vulnerabilities** and **opportunities**. It allows the policy-makers to face the **unknown** and best reduce their **uncertainty** when critical decisions must be made; (some emphasis added)*
- *To assist good governance by providing critical intelligence highlighting government **weaknesses** and **errors**. As guardians of peace, democracy and the Constitution, intelligence services should tell the government what they should know and not what they want to know.*

In the SA context, *the mission of the IC is to provide evaluated information with the following responsibilities:*

- *to safeguard the Constitution;*
- *to uphold the individual rights enunciated in the Bill of Rights;*
- *the achievement of national prosperity whilst making an active contribution to global peace and other globally defined priorities for the well-being of humankind; and*
- *the promotion of SA's ability to face foreign **threats** and to enhance its **competitiveness** in a dynamic world.* (White Paper, 1994)

The above context shows that SA's intelligence environment is tailor-made for an IRMF. However, SA needs to formulate the necessary IRMF doctrine and ensure proper implementation; as a history of failed implementation leaves some doubt as to the application of the framework. The HLRP states multiple incidences of management and members not complying with the necessary prescripts of the intelligence service. This was again re-confirmed by the 2021 JSCI report. For an IRMF to be successfully implemented, there should be some aspects that the IC comply with, as also indicated in the White Paper of Intelligence and the HLRP report. The intelligence processes that provide strategic intelligence products must be changed, and the emphasises must include several IRM principles, including multi-layered processes, communication between all structures with the same vocabulary, the use of specialised persons from internal and external environments, proper coordination, a holistic approach and well-trained personnel.

The departmental level in SA is fundamental to the success of good governance. If it fails, the policy-makers will not receive the necessary intelligence products for sound decision-making. The human factor at the departmental level is the biggest threat to the success of the intelligence environment in

the SA context. For example, Fraser's special operations unit had not followed these principles and did not comply with administrative rules and prescripts. Thus, no rogue unit must be allowed to operate without these control measures in place. These aspects need to be well researched, and the methodology regarding recruitment, development, and placement of these people must be done urgently. The human factor will play a significant role in implementing the IRMF, as RM concepts are known at the departmental level by management and among personnel. Therefore, how these aspects inter-relate will be reviewed in the following paragraphs.

4.4 The Evolution of Risk Management in South Africa from 1994 to 2020

SA has a rich history of RM which need to be analysed and evaluated to determine how well are these aspects implemented in the government of SA.

4.4.1 History of risk management - early developments in South Africa

The RM development in SA is not different to the rest of the modern world (Valsamakis *et al.,* 2005). Development started taking shape in the 1970s; and most broker houses (Alexander Forbs, First Bowing and Glen Rand MIB) were involved. The first RM statement signed by the chairman of the Board of Directors (1975) was the Barlow Rand Group chairman, which bonded the group to an RM programme (Young, 2008). Over the years, some associations were formed, namely the South African Risk Management Association (in 1975); South African Risk and Insurance Management Association (SARIMA) (in 1986); Society of Risk Managers (in 1990) and the amalgamated Institute of Risk Managers (IFRM) (in 2003) (Valsamakis *et al.,* 2005:23). RM was also integrated into the education environment of SA in the late 1980s. Programmes were presented by several universities, including the University of South Africa (UNISA), Witwatersrand, Stellenbosch, and Technicon SA. Thus, RM forms part of the curriculum of study at several universities today.

The international developments at the beginning of the 1990s initiated more development in setting standards for RM in all developed countries. SA has not fallen behind in this regard, and in 1992 the King's committee was formed to develop codes for Corporate Governance in the private and public sectors (Young, 2008:20-21). The committee issued four reports over the past thirty years (King I – IV). Valsamakis *et al.* (2005:23) state that RM's *focus has shifted from preventing and funding losses to managing all the risk in the organisation*. Different types of RM processes were implemented in SA by organisations based on all the different international and local codes and prescripts. However, even with all these methods and methodologies in place, RM could not prevent the financial crisis of 2008.

The SA government has also implemented RM rules and regulations in the public sector (National Treasury 2022). The government arranged that the banking sector and big financial institutions of SA comply with the internationally recommended supervision of their sectors issued by the Basel Committee on Banking, King Committee on Corporate Governance, and the Sarbanes-Oxley Act in the USA (Young, 2008). The King Committee analyses from an IRMF perspective; in the King II report, the necessary principles to implement an RM framework in the business environment are described. The King II Report (2002:76-77) mentions that *one of the mechanisms for managing risk is internal control. Internal control should be embedded in the company's daily activities in creating business plans, budgets, and other routine operational activities. There are, however, risks that do not make economic sense to control. In other words, the cost of control or mitigation exceeds the benefit thereof. Internal control is aimed at reducing risk to an acceptable level. Therefore, internal control is a process designed to provide reasonable assurance regarding the achievement of organisational objectives concerning:*

- *Effectiveness and efficiency of operations*
- *Safeguarding of assets*
- *Compliance with applicable laws*
- *Business sustainability*
- *Reliability of reporting*
- *Responsible behaviour towards stakeholders.*

The government is controlled through a legislative framework, which includes section 195 of the Constitution (1996), providing normative principles for public administration. Flowing from these principles, the Public Service Regulations promulgated in terms of the Public Service Act makes, among other things, provision for implementing a management framework for the Public Service, anchored on the principles of effective planning and accountability. Public service institutions need customised tools to comply with the defined planning requirements. For this purpose, RM can be regarded as a range of tools that support planning processes for service delivery.

Legislative prescripts on RM are contained in sections 38 to 42 of the Public Finance Management Act (PFMA) (Act 1 of 1999 as amended) and Chapter 3 of the Treasury Regulations (2001) for public service institutions. These prescripts deal specifically with the financial and fraud risk categories based on international and King codes. RM processes, responsibilities and even punitive measures for noncompliance are incorporated into the responsibilities allocated to accounting officers and audit committees. Per section 45 of the PFMA, all institutions' managers are responsible for adequately managing and implementing RM in their organisations. Furthermore, in terms of section 45 of the PFMA, the extension of the general responsibilities to all managers is a cornerstone in the institutionalisation of RM in the public service. It establishes RM accountability with all management

levels and does not limit it to the accounting officer or internal audit units. Notwithstanding these arrangements, government have institutions failed to prevent high levels of financial mismanagement.

The National Treasury Regulations' (2001) Chapter 3 (Regulation 3.2.1 and 27.2) instruct the accounting officers of the government institution to ensure that:

- A risk assessment is conducted regularly;
- Institutions identify emerging risks; and
- An RM strategy is drafted. This must:
  - include a fraud prevention plan;
  - direct internal audit efforts and priorities;
  - determine the skills required for managers and staff, to improve controls and manage risks;
  - communicate the strategy to all officials; and
  - ensure that the RM strategy is incorporated into the language and culture of the institution.

With the above information regarding the developments of RM in SA and the government, one can ask the same question as the HLRP - *what when wrong in SA*? The government was captured, and criminal activities were ramped up. The intelligence environment that needs to report and investigate these aspects is failing the government system. An IRMF can be implemented in the intelligence environment, however, the human factor hampers this framework. Therefore, an aspect of the intelligence environment which can direct implementation is the national security doctrine of the SA, which will be overviewed in the paragraph below.

4.5 National Security and a Strategy

The White Paper (1994) directs the drafters of a national security policy, strategy, and national interest, what was meant by the original Constitution (1996), and what national security should be in a democratic state. The White Paper (1994) states: *The maintenance and promotion of national security (i.e., peace, stability, development, and progress) should be a primary objective of any government*. Furthermore, in recent years, there has been a shift away from a narrow and almost exclusive military-strategic approach to security. Security in the modern idiom should be understood broadly to correspond with new realities since the Cold War era. These realities include the importance of non-military security elements, the complex nature of threats to stability and development, and the reality of international interdependence.

SA has identified these aspects and included them in its Constitution. The Constitution (1996: s 198) upholds these views: *(a) national security must reflect the resolve of SA, as individuals and as a nation, to live as equals, to live in peace and harmony to be free from fear and want* (a classic expression of

human security). Furthermore, the Constitution's section 198 prescribes that the following principles govern national security:

(b) The resolve to live in peace and harmony precludes any SA citizen from participating in armed conflict, nationally or internationally, except as provided for in terms of the Constitution or national legislation.

(c) National security must be pursued in compliance with the law, including international law; and

(d) National security is subject to the authority of Parliament and the national executive.

With this understanding, the intelligence and security cluster could draft the necessary policies, doctrine or research studies to provide these essential policies for implementation. The HLRP report indicates that the panel only had access to two national security strategies (2007 and 2013) prepared by NICOC. The 2007 draft document went to the NSC Directors-General meeting, where it stalled. However, the 2013 strategy went to Cabinet for approval on the 4th of December 2013. This copy was classified as top secret and, therefore, not available to the public or even within departments. There was no indication of a national security policy or interest documents in the cluster environment. These aspects leave ample space for misunderstanding by the different role-players and policy-makers.

Furthermore, the HLRP indicates that the 2007 National Security Strategy (NSS) extensively consulted with the public and Parliamentary environments before the final draft was approved. The 2013 top-secret document was not provided to the security cluster for comments, leading to several complaints by the SANDF. Therefore, reports on the NSS (2013) indicate that the document's classification limited the document's purpose and distribution.

Daniels (2019:1), the Africa Centre for Strategy Studies, and the HLRP recommend urgently drafting an NSS. They believe in *an urgent need to develop a cogent, integrated security strategy from the elements within the cluster departments*. The international security agenda is shifting to the full range of political, economic, military, social, religious, technological, ethnic, and ethical factors shaping security issues worldwide. The new thinking and changes in security have the following key features, which should form an integral part of the philosophical outlook on intelligence:

- *Security is a holistic phenomenon that incorporates political, social, economic, and environmental issues;*
- *Security policy objectives go beyond achieving an absence of war to encompass the pursuit of democracy, sustainable economic development, and social justice; and*
- *Regional security policy should seek to advance the principles of collective security, non-aggression, and peaceful settlement of disputes.*

The broader and modern interpretation of the nature and scope of security leads to the conclusion that security policy must deal effectively with the broader and more complex questions relating to the vulnerability of society. Therefore, national security objectives should encompass the basic principles and core values associated with a better quality of life, freedom, social justice, prosperity, and development.

These changes in national security make it even more critical to define the concept as in Chapter One of this dissertation. National security is defined broadly, taking its cue from the IWGNS (2013): *National security is the first and most important obligation of government. It involves not just the safety and security of the country and its citizens. It is a matter of guarding national values and interests against internal and external dangers – threats that can potentially undermine the security of the state, society, and citizens. It must include not just freedom from undue fear of attack against their person, communities or sources of their prosperity and sovereignty but also the preservation of the political, economic and social values, respect for the rule of law, democracy, human rights, a market economy and the environment, which are central to the quality of life in a modern state. (*IWGNS (2013:3)

An IRMF can be implemented in the environment if clarity is given regarding a national security policy, strategy and SA's interests. These documents will be needed to direct and influence the IRMF from an executive level. Most of the intelligence and security cluster departments' planning and objectives will derive from these documents. The external threats, risks and vulnerabilities that will be identified must be more manageable because the cluster will have better direction and understanding of the policy-makers' views on these essential aspects.

4.6 Conclusion

The analyses from an IRMF perspective in this chapter clearly show that an IRMF can be implemented in the intelligence and security environment of SA. Over the years, the legal framework and structures have been very well-drafted and directed the intelligence, police, and military environments to operate in a democratic state with its principles and rules. Notwithstanding all these arrangements, the human failure of the system is evident. Most of the reports were very weak in pinpointing the real problems in the intelligence environment. The personnel are the biggest problem, not the legal framework or structures in the IC. As pointed out by the HLRP and the media reports, some individuals indicated the abuse of the environment by executives and senior personnel to benefit ANC leadership and themselves.

With the above background, one would like to soften the impact of this personnel misbehaviour and total disregard for the rule of law, even if the arguments of Gill and Phythian (2018:29) are included.

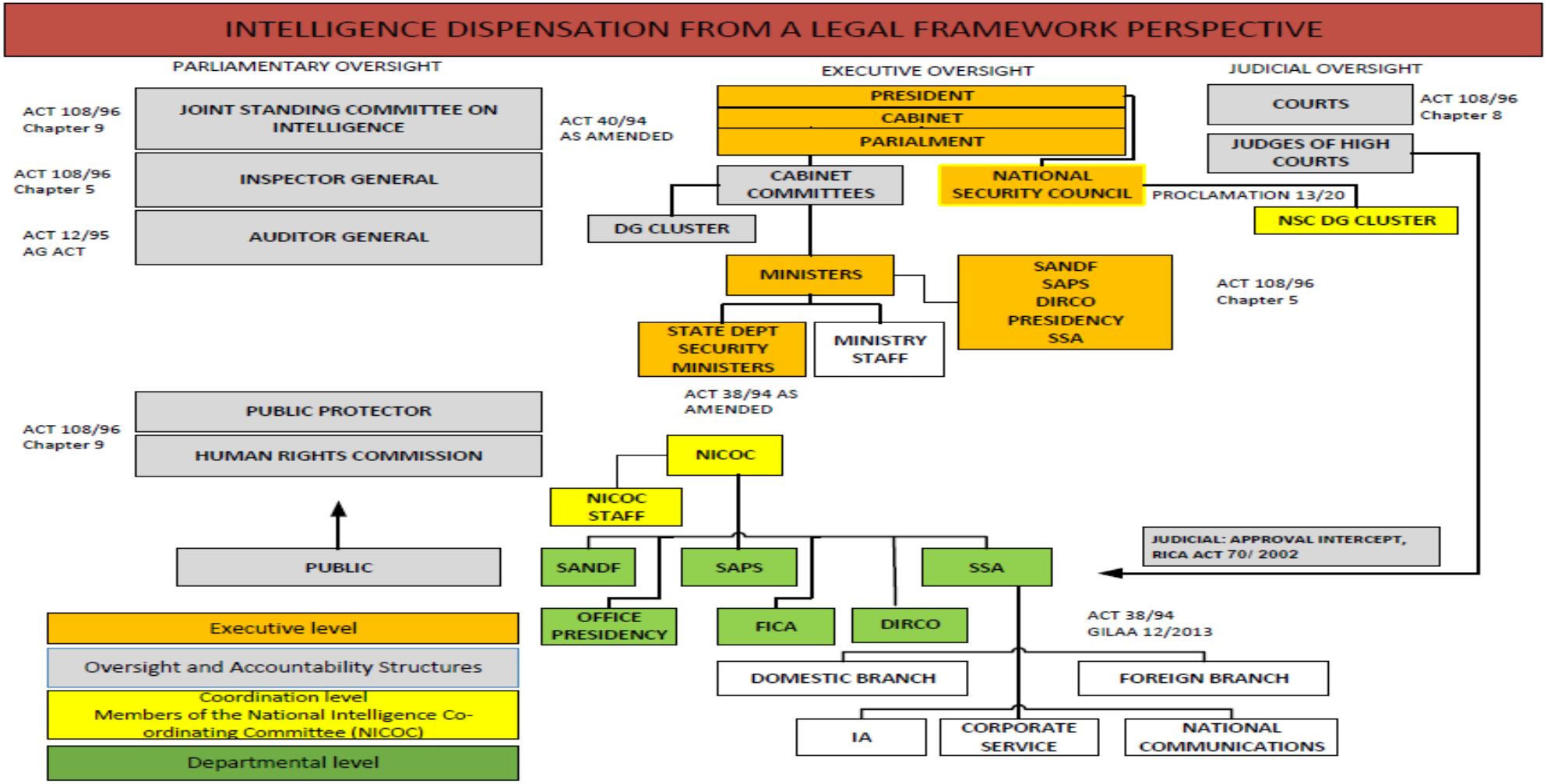
They argue that *within the broader context of democratising agencies in former authoritarian regimes, emphasis has been placed on the professionalisation of intelligence officials. The professionalisation involves replacing loyalty to a party or ideology with loyalty to a notion of national security and public safety that reflects a genuine assessment of a country's needs rather than merely the security in the office of a specific faction.*

The intelligence officers in the intelligence and security cluster have not lived up to these codes, as reflected in the above analysis of the intelligence environment. Reports indicated severe maladministration, corruption, illegal units acting above the rule of law, and people at executive levels ill-qualified to manage those positions. There were reports of non-compliance with the basic regulated feedback to Parliament and its committees.

This chapter found that the legislative framework and structure complied with the Constitution, the national legislation controlling the intelligence environment, as reflected in Figure 20 below. The IC needs to have the will, knowledge, and training of an IRMF to implement it successfully in SA. In the words of Arad (2008:44) *this is somewhat surprising, given that practitioners of intelligence and intelligence management are trained in probability thinking and, in need, to use various tools in assessing situations concerning early warning. The modes of thinking about RM and related concepts are especially well suited to the surprise-attack problem.*

In the SA context, intelligence services are trained in RM, which is enforced through the Acts and regulations in the country. However, these services do not apply the Acts and regulations in their institutions. When management is non-compliant, no action is taken against them by the ANC; their wrongdoing is overlooked and instead they sit at home and are paid full salaries. Arad (2008:44) furthermore states that a *close examination of the various elements in intelligence work discloses that intelligence organisations already tacitly implement fundamentals of risk assessment and management. In addition to probabilistic measurements, evaluation of risks and the use of scenarios, explicit risk-control and risk-management tools are widely used, such as backup systems and risk reduction via diversification and redundancy. Nevertheless, all these elements have not coalesced into a comprehensive RM doctrine for intelligence.*

These aspects are covered in the National Treasury's 2001 regulations and the substituted guidelines for the implementation of RM in government institutions. Therefore, one can not only ask the question of *What went wrong but also How could it go wrong?* The benefits of IRMF will be an essential management tool for the future of intelligence in SA, as it will nudge the government to take action against these wrongdoers. Thus, the next chapter will explore how these tools function in the intelligence environment.



Source: Adapted from SSA Ministerial website (2014)

Figure 20: The intelligence structures of SA 2020

CHAPTER 5: THE APPLICATION OF AN INTELLIGENCE RISK MANAGEMENT FRAMEWORK FOR SOUTH AFRICA

…create a more adaptable organisation, which first recognises change and uncertainty, and secondly uses it creatively to its advantage (Van der Heijden, 2005:1)

5.1 Introduction

The IRMF constructed and reconstructed in the previous chapters (See Figure 15) will be operationalised within Chapter Five. Throughout history, intelligence and security agencies have been criticised and questioned because of serious failures, which led to many lost lives and the economy collapsing. These surprises tempted governments worldwide to appoint commissions or review boards to investigate the intelligence and security agencies' structuring, functioning and processes to overcome these failures. The analysis processes were under scrutiny because they could not identify the delicate signals to forecast or identify these threats, risks, or vulnerabilities in time. These commissions have not considered the full processes of intelligence, current intelligence collection and analysis processes, thus they have no proper review of the work their intelligence agencies are doing. This research has studied and conceptualised an IRMF for SA (as depicted in Figure 15) and in this chapter, the implementation of the processes flowing from this IRM process will practically test or evaluate the framework to determine if it could be implemented in the SA intelligence environment.

This chapter will mainly focus on SA's stability/instability from a political perspective as an area of interest. In the past fifteen years, frequent reports regarding SA's economy and political instability have appeared in the media, as well as in academia. The country has experienced poor social-economic growth and even a financial downgrade of SA due to violence, poor governance and deficient policies. These paradigms will be explored, described, and explained. The emerging economy, governance, society, and security of SA, which was under pressure due to global economic changes, poor financial management and the downgrading of SA's economy, violent protests in the country during 2021, high crime rates and specifically violent crime, will be reviewed and analysed.

Chapter Five plans, develops, and builds scenarios to critically assess SA's instability situation compared to other BRICS, IBSA, and CIVETS countries, as well as African countries, which are viewed as the most successful and well-governed African economies. This analysis will assist and indicate which methods and analytical tools can be used in the IRMF. Furthermore, this chapter will develop categories for implementing an IRMF applicable to SA. In this analysis, internationally known institutions' data will be used. Through quantitative, qualitative, and comparative analysis, a

risk/instability profile from an IRM perspective will be constructed, leading to futuristic scenarios that will show SA's future development path. Moreover, Chapter Five will assess which techniques and methods of the conceptualised IRMF depicted in Figure 15 are more applicable and effective in building plausible scenarios or security risk analysis assessments, providing the policy-maker or client with better recommendations.

5.2 The Construction of a Futuristic Scenario Analysis for Use in an Intelligence Risk Management Framework

To construct scenarios, it is essential to follow specific steps in the planning and building of these scenarios. The focus in this chapter will be SA; therefore, specific information regarding SA is needed to formulate these scenarios. This chapter section will analyse these aspects and conclude with plausible scenarios.

5.2.1 Background regarding South Africa

SA is viewed as an emerging market by the most prominent grading agencies (Moody's, Standard & Poor's, and Fitch), WB, IMF, StatsSA, researchers, and academics. Furthermore, SA is blessed with an ample supply of resources (gold, platinum, chrome, manganese, vanadium, coal, and diamonds) and well-developed communication, financial, energy, legal and transport sectors, notwithstanding poor governance of these sectors by the regime. In the stock exchange, SA is ranked 17th, among the top in the world (United Nations [UN], SSE, 2022). Given the above, the broad macro-political risk profile of the country has changed fundamentally and worsened substantially from 2008 to 2022 (Neethling, 2021). In this context, the country's political risk profile must be considered a matter of serious concern from an IRM perspective. For additional information on this issue, see IMF (2021) and StatsSA (2018; 2021) and WB (2018).

Therefore, the question can be asked why and what went wrong from 2008 to date. Why specifically is SA as a country so unstable, and is there no proper development and growth? To determine these aspects, one needs to understand stability and instability from an African perspective and, through futuristic scenario processes, develop compelling scenarios for SA.

5.2.2 What is the stability or instability of a country or state?

The concepts of stability and instability in political science are described by Hurwitz (1973:449) as fuzziness, and there is no clarity regarding their *definitions, operationalisation, and measurement*. The author states that *the concept of stability means all things as various individuals attempt to*

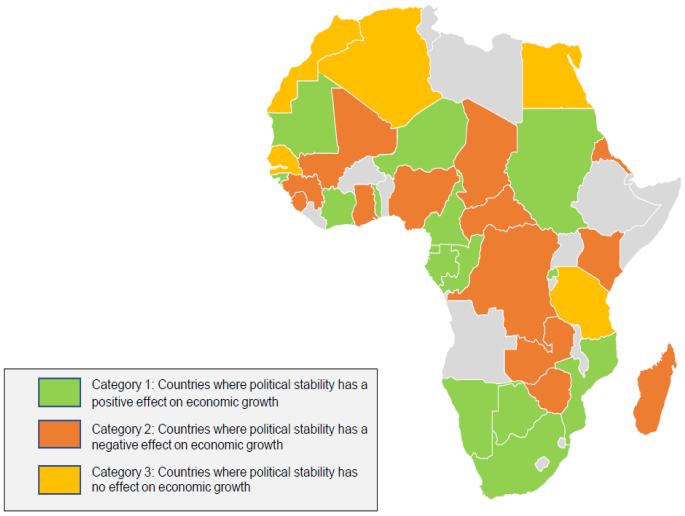
measure the degree or amount of 'political stability' present.... Hurwitz, furthermore, states that political stability is assessed against five particular variances, which include: *(a) the absence of violence; (b) governmental longevity/duration; (c) the existence of a legitimate constitutional regime; (d) the absence of structural change; and (e) a multifaceted societal attribute*. From an African perspective, Ake (1974:347) explains that instability of 'new states' (decolonised states after WWII) occurred due to *…usually stress one or more of five related factors: cultural heterogeneity, low regime legitimacy, lack of coercive power, economic backwardness, and structural simplicity*. Ake (1947:500) therefore, defines stability as *Political stability is the regularity of the flow of political exchanges; the more regular the flow, the more stable the polity*. These views of stability form part of the primary development of opinions over the years regarding stability and failed states. All indication is that these types of states do not attend to the basics regarding governance, administration, and development in their respective countries. Derouen and Goldfinch (2013:499) indicate that *for these countries, performance on developmental indicators is abysmal and often regressing; governments are predatory; infrastructure can be virtually absent; human rights are abused, corruption, criminality and violence are epidemics; warlordism can be pervasive; terrorism, war, piracy, and refugees are exported; and societal collapse is apparent or imminent.*

Derouen and Goldfinch (2013:499-500) also acknowledge that these aspects can change, and states may *exist on a continuum from variously stable to highly unstable, failed or collapsed*. They opine that history, culture, agency, context, and contingency variances influence countries' stability or instability. These views and understandings, as seen above, bring more clarity to the fuzziness, definitions, operationalisation, and measurement regarding stability and instability in political science. In fact, Derouen and Goldfinch (2013:501) approached stability with a more positive and understandable approach to fuzziness regarding these phenomena: *stable states are characterised by government capacity, legitimacy, a legal/rational state, democracy and human rights, and development and economic integration will ensure stability*. These aspects apply to the SA context. With these aspects clarified, futuristic scenarios can now be built and planned.

5.2.3 Step One: Identify focal issues regarding stability and instability in South Africa

The above considered, it is essential to take note of the research done by Chtouki and Raouf (2021:50-51) regarding peace and stability and the impact of these phenomena on states in Sub-Saharan Africa. These findings are essential for understanding the SA context of instability. They view the African continent as one of the most unstable areas in the world, establishing that instability and peace influence these states' socioeconomic growth and good governance. These phenomena create challenges for African leaders in particular; therefore, they were categorised into three specific categories:

- **Category 1:** Includes ±45% of the countries whose gross domestic profit (GDP) will be positively influenced by stability. Their findings correlate with most other studies regarding stability and the influence on socioeconomic growth. Therefore, these countries show good socioeconomic and development growth with the absence of instability aspects influencing their growth. The countries in this category are Botswana, Mozambique, and Namibia, which are relatively politically stable and have shown socioeconomic growth. The stability that these countries can positively influence neighbouring countries like SA, which is unstable and experiencing low growth and development, specifically from 2008-2022. Furthermore, SA needs to be analysed to determine the reasons for its poor performance in the group/category.
- **Category 2:** Includes ±35% of countries in Africa's central and western regions that were negatively influenced by instability. These countries have low levels of political stability and experienced much geopolitical turbulence during the 20th century. These countries have experienced low socio-economic growth.
- **Category 3:** Includes ±20% of the northern African countries. All indication is that political stability does not affect their socioeconomic growth. These countries include Morocco, Egypt, and Algeria, which were relatively stable from an African perspective. Most of these countries have effective control policies. Thus, the absence of stability in these countries has less impact on their economic and governance development. Figure 21 below shows their findings and the three specific categories in which the different African states can be rated.



Source: Reproduced from Chtouki and Raouf (2021:50-51)

Figure 21: Mapping the effects of political stability on short-term growth

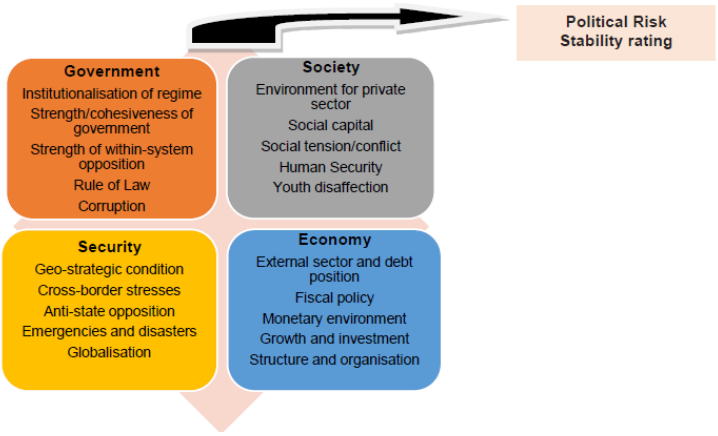
These findings show that it is imperative to understand the reasons for instability in countries from an IRM perspective and precisely the phenomena that influence SA. Bremmer (2005:1-3) explains that political risk is the primary phenomenon influencing the stability of a country. Political risk is defined as the political impact on government (governance, society, security, and economy).

Political risk includes everything that can influence the political environment negatively or positively, which determines stability. Political risk analysis is subjective and can include trends that leaders should focus on, such as nuances of society, individuals, groups, and personalities. Moreover, the political risk environment can also contain hard-to-quantify factors which need to be included in an analysis. These factors/trends will influence the ongoing narrative within the analysis from a historical and regional context.

In SA, certain political risks persist while new ones arise, such as the political uncertainty that has risen over the past few years (2016-2022) due to instability. For additional information on this issue, see IMF reports on the website (2006-2022), WB reports on the website (2000-2019) and Neethling (2012; 2016; 2021). According to the Minister of Finance's (SA) Medium Budget Policy Statement in October 2022, the uncertainties in SA's external environment are considered a significant source of risk for SA's economy and governance. Nevertheless, according to the IMF (2006-2020), SA's internal risks have been on the rise, such as SA's current rising account deficit, disappointing and declining mining outputs, state-owned entities (SOEs) (Eskom, Rand Water, South African Airways, DENEL, Post Office, Landbank) that do not deliver quality services and are in serious financial ruin, and high levels of corruption. Thus, political uncertainty, threats, risks, vulnerabilities and opportunities will be identified to overcome the instabilities hampering the development and growth of SA. These aspects will be analysed through a framework of the Eurasia Group (Keat, 2008), which was identified as the foundation for the assessment below.

5.2.4 Step Two: Eurasia Political Risk Index – Framework to evaluate state stability

According to Keat (2008:265), the Eurasia Group's Global Political Risk Index (GPRI) systematically tracks various factors that constitute country stability. The GPRI serves as a comparative framework for identifying trends within and between countries, whilst anticipating the likelihood of crises (see Figure 22 below). The index defines stability as its conceptual opposite, instability – or proneness to a crisis. Unstable states are, thus, prone to and most likely to experience crises; stable states are not prone to and least likely to experience crises. The index defines crises as major systemic dislocations that threaten the survival of governments, regimes, or states. These include, but are not confined to, revolutions, rebellions, civil wars, and regime breakdowns. This study will use these variables and framework as the foundation for its analysis. The fundamental forces influencing SA's instability are government, society, security, and the economy. The GPRI variables could be depicted as follows:



Source: Adapted from Keat (2008:265)

Figure 22: The variables of Eurasia Group's GPRI

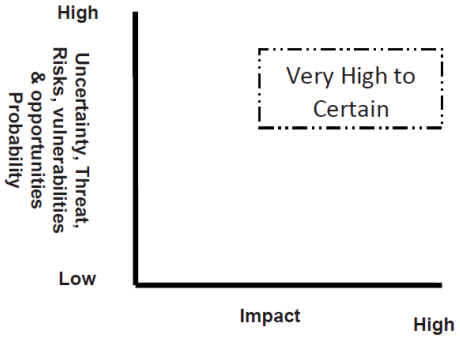
5.2.5 Step Three: Determine the driving forces which can change aspects of the South African environment through these four variables

The comparative framework of Eurasia Group consisted of four variables as indicated in Figure 22, which this study will use to analyse the driving forces behind the instability of SA (Keat, 2008). These variables (governance, society, security and economy) will form the foundation for this analysis, and international research institutions and agencies' data will be used. The most common way to measure a country's risk is its sovereign rating. A sovereign rating is compiled by analysing various qualitative and quantitative factors. Sovereign ratings are calculated and provided by the leading global rating agencies, namely WB, IMF, Eurasia Group, Bloomberg, UN, Moody's, S&P, and Fitch. The factors of influence on these four variances will differ because of SA's changing environment. Therefore, different analytical examples used in the assessment were considered to ensure that broad capturing of data occurred, to provide a better-balanced picture of the SA landscape. These aspects will also direct the rating trends in the SA context.

5.2.6 Step Four: Rating trends in the South African context from an Intelligence Risk Management Framework perspective

In an IRM process, all aspects of uncertainty, threats, risks, vulnerabilities, and opportunities need to be rated according to their impact on the political system and what can be done to soften or neutralise their impact. This type of analysis is usually done using a two-axis graph, as reflected below in Figure 23. Cronje (2014) describe the graph and how it is used to determine these impacts. The first axis indicates the uncertainty, threats, risks, vulnerabilities, and opportunities, with the other axis indicating the impact of these variances on the political system. For example, state capture by many individuals and companies in SA will be a high threat and have a very high impact on governance and the economy (indicated by the text box in the graph below). This process will

provide the analyst with the necessary information to determine the high trend according to impact for an analysis. This also assists the next step to select scenarios.

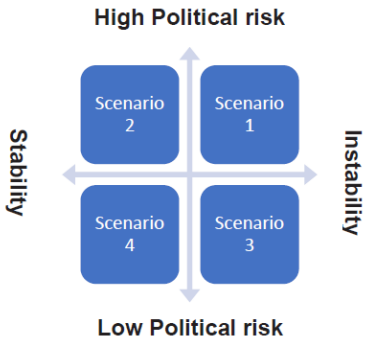


Source: Adapted from Cronje (2014:49)

Figure 23: Graph indicating uncertainty, threats, risks, vulnerabilities, opportunities; their probability of materialising and their impact

5.2.7 Step Five: The selection of scenarios

According to Cronje (2014), the fifth step is to produce a matrix based on the two most important probabilities/trends identified in the impact (uncertainty, threats, risk, vulnerability, and opportunities) graph shown above. These two trends then become the axis of a matrix, and the scenarios are developed in the quadrants formed by these axes. For example, if political risk and stability are identified as the two most important and probable uncertain/risk trends influencing the future of a system, the matrix would be constructed with these two trends as its axis (Figure 24).



Source: Adapted from Cronje (2014:50)

Figure 24: Matrix indicating the futuristic scenarios

The matrix assists this study in developing four scenarios for SA. They are reflected hereafter in paragraph.

5.2.8 Conceptualise a framework for risk layers on the SA's political instability/stability index

To conceptualise a framework in this paragraph, all the forces which stabilise or destabilise SA much be identified and described. This study uses a combination of Eurasia Group (2010) and Schwartz's (1996) methods to analyse these variables. Schwartz (1996:100) looks at a familiar list of driving forces to determine from these categories the different layers to formulate their scenarios - *Society, Technology, Economics, Politics, and Environment*. Combining Schwartz's driving forces with those aspects of the Eurasia group's variables in a SA context will then be reflected, as shown in the table below. Some of the combined possible outcomes have also been shown to direct the analysis and give some indicators regarding the forces influencing instability or stability.

Table 10: Combined table of Eurasia Group and Schwartz for SA

Eurasia Group variables	Schwartz Driving Forces	Outcomes
Governance	*Politics*	Policies, Prosecutions, Zondo Report, Factions, Political violence, Law and Order, Polity.
Society	*Society*	Education, Unemployment, and Health, SA's weak growth performance has contributed to high unemployment levels. Poverty and inequality have increased due to their correlation with unemployment.
Security	*Environment*	Poor management, Sabotage, Smuggling, Criminal anarchy, Energy Security, Water Security, Food Security,
Economy	*Economics, Technology*	ESCOM, Electronic broadband, Budget, Corruption, Reforms, SOEs

Source: Researcher's construct

The above table gives more clarity regarding the main variances that the chapter needs to focus on to determine the two axes, stability/instability and political risk, high or low, as described above. These variances will now be further expanded and analysed.

5.2.8.1 Governance

The first main variance is governance, and from an IRM perspective, one needs to understand what governance is and how it influences the state. In this context, the United Cities and Local Governments Asia-Pacific (2021) states that *governance is a concept that has been around for years and is commonly used by many people. There is almost no consensus on the official definition of governance because its use often depends on the intended purpose and the people involved* [own emphasis].

According to the UN (2014:1), it can be defined as follows: *governance refers to the activities of all political and administrative authorities to govern their country*. Meanwhile, the IMF (2022) states *governance is a country's management concept, including economic, policy, and legal aspects*. The WB (1992:1) became the first international institution to adopt the concept of *good governance as*

the way power is used to regulate a country's economic and social resources for development. This study will view good governance as the way power is used to regulate a country's management concept, including governance, society, security, and economic resources for development.

With the above definition in mind, the Mo Ibrahim Foundation's (n.d.) data were analysed to determine how good SA's governance is. The IIAG was established in 2006 and provided the most up-to-date quantitative data on African countries' governance. The data were collected by experts from several countries' institutions and annually assessed to provide these reports and indexes regarding African governments. These reports and indexes provide a rating and comparison of 54 African countries. The focus of this dissertation will be on SA, and comparatives will be made between SA and other countries to show the differences due to the political risk SA is facing, destabilising the country. Furthermore, the qualitative data will be analysed, and problem areas that influence the SA political environment will be identified.

According to the IIAG 2020 scores, ranking and trends, SA is ranked sixth out of the 54 African countries assessed. Despite their scores going up, SA's ranking had fallen from fifth to sixth since 2000. Schwella (2017:231) identifies that *SA is one of eight countries to have remained consistently in the IIAG top 10 since 2000 - along with Botswana, Cape Verde, Ghana, Mauritius, Namibia, Seychelles, and Tunisia*. These findings show that SA applies and manages some aspects of good governance. The questionable assessment of SA governance is why the country does not perform better or keep its scores, ratings, and trends higher. Schwella (2017:231-232) states that *Given the leading position of SA in many other facets of governance- related activities – such as banking, trade, commerce and specifically academia as related by high rankings of SA academic institutions in global assessments*. There were 14 universities under the top 2000- 2022/23 rankings (US News and World Report, 2022). SA's assessment shows a disappointing governance performance, which is currently rated sixth on the African continent. The IIAG assessment of SA shows the variances influencing these ratings of SA:

- Security and safety (human trafficking and forced labour, crime);
- The rule of law and justice (law enforcement is poor, property rights questionable);
- Accountability and transparency (undue influence on government);
- Anti-corruption (high levels of corruption in public and private sectors, state institutions cannot put control mechanisms in place and maintain these control measures).

The variances mentioned above prove already-identified aspects by academia, researchers, and analysts regarding the poor governance of the SA government. The media regularly requests that the government control these aspects but to no avail. For additional reading, see Schwella (2017) Chapters 7–9 and IRR (2016). These aspects do not only bring the scores and ratings down but

influence society in SA, and more negativities have been observed over the past decades, reflecting negatively on investors. Crime has become a severe problem due to high unemployment and living costs, with no growth in the economic sector. Moreover, the IIAG index (2020) reports SA's governance aspects as follows (out of 54 countries assessed):

- Places SA sixth overall;
- SA's average score of 65.8 out of 100 is higher than the African average but SA shows a drop of -0.9 points between 2010-2020;
- Ranks SA's highest overall position in the category of Human Rights at second;
- Ranks SA's lowest overall position in the category of Safety and Rule of Law at eighth;
- Ranks SA's lowest overall position in the subcategory Public Management at 22nd; and
- Ranks SA again at the lowest overall position in the subcategory Personal Safety at 41st.

This assessment of SA governance shows that SA is slowly deteriorating in the African governance context. Thus, SA must enhance their focus on these variances as there are opportunities to correct them. The ANC regime must be held accountable for the flawed government system failing the country and its society and should request SA universities to assist in the effort to improve poor service delivery and management. There must be consequent action against those government officials who are not performing their work correctly through Parliament. Cutifani's (2012:5, in Neethling, 2014) statements are important in this regard: *government should get the basic functions of government working*. Fortunately, the IIAG ratings and reports show that SA is doing some things correctly, and there are variances that the government can build on in which SA has a leading position, such as:

- Strength/cohesiveness of government; and
- Human development, notwithstanding the poor performance in the health sectors, which will be analysed later in this chapter.

The second variable which needs to be focused on is **Polity.** This variance is a very dominant aspect of governance in SA. A one-party regime, the ANC, dominates the political environment. Since 1994, the ANC has won every election, and they did not need any approval to be a legitimate government (see Table 11 below) as SA citizens voted for them. Nevertheless, they showed that they did not need any authoritarian measures to retain power over the years. Neethling (2017:39) explains the concept of authoritarianism; it *pertains to a lack of democracy, ranging from totalitarianism to authoritarianism, which may lead to discontent. Violence usually lies very close to the surface. This indicator includes rigid control over citizens, even though sometimes superficial control*. The state capture and Zondo Commission reports show that these aspects have led to violent and dysfunctional governance. During the Zuma era, there were increased indications of authoritarianism in the rule of the ANC regime. In addition, the President (Zuma) controlled these

aspects, as the Institute for Security Studies (ISS) (2022) report shows: *Former president Jacob Zuma controlled this infighting, largely through patronage and repression*. These aspects will create a threat to the stability of the SA political environment; as ISS (2022:1) determined that there is a link between service protests and ANC activities in the country.

The above knowledge about SA helps to understand the political landscape as a one-party dominated democratic state without a solid formal opposition that could act as a serious political contender at the polls. Neethling (2017:39) states that *despite its nominal constitutional democratic states, the ruling party is still prone to sink into arrogance and corruption and confuse the state's interests with that of the party*. These aspects have materialised in SA with high levels of corruption; worryingly, former President Zuma stated that the ANC would rule *until Jesus comes back* (Mail & Guardian, 2014), even though the Zondo Commission's findings state that several elites of the ANC are guilty of corruption and criminal acts. The question in this regard is whether the ANC will have the will and accountability to act against these members. The Daily Maverick (2022) refers to President Ramaphosa's feedback on the Zondo Commission report: *But his public statement on Sunday night also demonstrates that he is failing — at least for the moment — to act against individuals he appointed and against whom the commission made findings*. These aspects show that the ANC's dominance creates a severe risk to the country's stability. These actions, as described above, will influence SA's political landscape. Should the ANC lose the next election in 2024 (or lose control and need to rely on coalitions), SA will be at risk of instability.

Cronje (2020), a well-known scenario planner and researcher, used well-formulated probabilities to indicate what can happen in the future political environment. Should the ANC lose, as mentioned above, Cronje (2020:129) states that it could decide to act in the following way(s):

- *The ANC suffers further losses of support and reincorporates the Economic Freedom Fighters (EFF);*
- *The ANC sees its support slip to below 50% and secures a majority with the support of smaller parties, or a broad coalition of opposition parties conspire to keep the ANC out of government;*
- *The DA wins outright as early as 2024, but more likely in 2029 or even 2034;*
- *The ANC builds a coalition with the DA;*
- *The DA consummates its marriage with the EFF and moves hard left; and*
- *A new political player enters the arena and becomes influential in determining the trajectory of future coalitions*.

Currently, Cronje's (2020) political outcomes are all possible. Political opposition has grown in the past decades and the ANC's main opposition lies in the Democratic Alliance (DA), and the third

largest party, the EFF, which has had some growth. Major political parties' election results from 1994-2019 are shown in the table below.

Table 11: National Elections Results SA: 1994 to 2019

National Elections Results in SA: 1994 – 2019, Top Three Parties						
Party	**1994**	**1999**	**2004**	**2009**	**2014**	**2019**
ANC	62.7%	66.4%	70%	65.9%	62.2%	57.2%
DA (DP)	1.73%	9.6%	12.4%	16.7%	22.2%	20.8%
EFF					6.35%	10.79
IFP		8.58%	6.97%	4.55%	2.4%	3.38%
COPE				7.42%		

Source: Researcher's construct, data sources from IEC

From 1994 to 2019, main parties have changed; however, the ANC has remained a viable, contesting party. The 2019 election saw the two top parties, the ANC and the DA, decline, and the EFF gained more than 4% support. Since 1994, the DA is the only other party which has won (and held) a provincial election (2009, Western Cape). However, the chance that the ANC could lose its hold due to infighting is considered a political risk, as it could open the door to its attempts to destabilise any opposing coalitions (ISS, 2022:1). For example, the 2019 local government elections (LGEs) brought exciting developments to SA's political environment. The dominant ANC party obtained a result lower than 50% for the first time. They did not secure all the main metro cities in Gauteng, and opposition parties formed coalitions to rule in some cities; however, the ANC tried to fight back by making secret arrangements and reclaiming control (but failed). The ANC had also called for the postponement of the LGEs under the guise of Covid-19 safety concerns (also failed). Their loss of control was not surprising, considering the *corruption scandals within government, an economy in which high levels of unemployment have surged, scheduled electricity blackouts occurring almost daily, and a generally poor record of governance at a local level* (Cronje, 2020). The main opposition party, the DA, had thus far been unable to capitalise effectively on the ANC's decline; new, smaller parties emerged and old nationalist-type parties gained votes during the elections (results in Table 12). The election's outcome brought coalition government politics to the table, which created instability as these parties failed to liaise properly, leading to break-ups; thus, SA needs more knowledge surrounding coalition ethics and rules.

Table 12: LGE results in SA: 2019

LOCAL GOVERNMENT ELECTION RESULTS: 2019			
PARTY	**COUNCIL LEADING**	**COUNCIL CONTROL**	**% SUPPORT**
ANC	167	122	45.59%
DA	24	12	21.66%
IFP	16	9	5.64%
NFP	1	0	0.5%
ICOSA	1	0	0.09%
EFF	0	0	10.31%
VF PLUS	0	0	2.34%
ACTIONSA	0	0	2.33%
PA	0	0	0.97%
ATM	0	0	0.57%
UDM	0	0	0.47%
OTHERS	0	0	7.63%
IND	0	0	0.73%

Source: Researcher's construct

The 55th ANC elective conference will determine SA's political future, as it will determine how long until SA can be considered a failed state. If the more radical faction in the ANC wins the election, SA policies will quickly change to accommodate nationalisation. If the current leadership maintains their positions and President Ramaphosa gets elected for a second term, the status quo will be followed, prolonging our deterioration to 2029. If the current leadership wins by an extended margin and they apply reforms, the situation in SA can improve (Cronje, 2020).

The **Rule of Law** is one of the sub-variances under governance which need this study's attention. The IIAG (2021) and the UN Human Development Index (HDI) (2021) indexes indicate that the SA government is not governing these areas very well. Daily reports of crime and statistical data confirm this poor governance. For example, the President's Expert Panel assessed the July 2021 violent protests and looting. The report (2021:50-51) indicates that *the Security Services need to strengthen their technological capacity as well, and all technology equipment possible to secure the state must be legally applied. The executive must also be better coordinated and aligned, and the NSC must take the lead in security policy coordination. NICOC's role in strategic intelligence coordination needs to be affirmed*.

This statement reflects what is happening in the broader government environment and paralyses government service delivery. The government needs to enhance their attention to speedily resolve legislative compliance in line with the Constitution. The Financial Action Task Force (FATF) (2019), which sets standards and promotes the effective implementation of legal and operational measures for combating money laundering, terrorist financing, and financing of weapons of mass destruction internationally, reported SA's non-compliance with standards and legal frameworks. If the responsible government departments do not meet these requirements in time, SA faces a grey-listing. The government must provide feedback to FATF by the end of December 2022, and all indications are that SA will not meet this deadline (thus, being grey-listed). As reported by Business Maverick (2022), a private research company *Intellidex estimates that the economic impact of grey-listing could be limited at under 1% of GDP lost from higher costs to international transactions over 18 to 24 months if SA is perceived to be far advanced in addressing concerns of the FATF report. However, this shifts to an estimated up to 3% of GDP lost from higher costs to international transactions over five years, with a gradual recovery if the country is perceived to be slow and unwilling to take the required actions. The economic impact would primarily arise from increased cross-border payment transaction costs and the general reputational impact.*

The FATF report also indicates that SA members are poorly trained, with no experience in international cases in this field. BusinessDay's (2022) article by Ensor, states that *Treasury acting DG Ismail Momoniat says SA has made 'significant and real progress' in meeting the requirements*

laid down by the FATF to avoid grey-listing. This grey-listing will pose a severe risk to financial payments by banks, companies, and the government, as well as prevent SA security services from operating effectively. In Chapters Three and Four, this study indicated instances where the country's intelligence agencies have not yet implemented commissions or panel recommendations.

BusinessTech (2021) reports that *SA's spy problems are well documented and were brought to the fore in the 2019 court case challenging the constitutionality of RICA*. Additionally, the investigative journalist group amaBhungane challenged RICA's constitutionality, by taking the government to court regarding a journalist being spied on (the Zuma Spy Tapes saga). The case was only brought to court in 2019 and the High Court ruled as follows (BusinessTech, 2021):

- *The act fails to adequately prescribe the procedure for notifying a person whose information has been intercepted;*
- *The act fails to adequately prescribe the proper procedures to be followed when state officials are examining, copying, sharing and sorting through data obtained through interceptions;*
- *The act fails to adequately address situations where the subject of surveillance is either a practising lawyer or a journalist.*

This ruling was upheld by the Constitutional Court in 2020, giving the government 36 months to rectify the issue. When drafting this dissertation, no indication was found in the media that the government had complied with these court rulings. Again, it is clear that the government has a slow response time to issues of 'law and order' if they comply at all.

To summarise, the National Planning Commission's diagnostic report (2011-2018) shows that the National Development Plan (NDP) was not implemented. The Commission stated that, at best, the NDP could not be adequately evaluated because its priorities are not in line with national priorities. Schwella (2017:262) indicates that the commission's report can ascribe the government's poor performance to three aspects: *Organisational instability and the political-administrative interface; Uneven capacity leads to uneven performance; The erosion of accountability and authority structures*.

These aspects above confirmed the findings of this section of the study regarding non-compliance. The SA government's ability to render services is deteriorating at an alarming rate, and the government needs to address it. The Commission's report also confirms this study's view that universities and academic institutions must assist in solving service delivery issues through education and training (National Planning Commission, 2018:3).

5.2.8.2 Society

The second main variance under this section will focus on **Society**. Study.com (2022) indicates that s*ociety in political science is the group of people within the region of a political system. These are the people affected by the decisions and actions of the government. In authoritarian and communist nations, government controls the economy and society. In a democracy, society is responsible for running the government. Furthermore, a society is a group of individuals involved in constant social interaction, or a large social group sharing the same spatial or social territory, typically subject to the same political authority and dominant cultural expectations.* [own emphasis]

Schwella (2017:229-230) describes SA society as: *…characterised by an active, often activist, civil society*. Several civil society institutions and bodies are actively involved in SA. The government needs to serve these people through value-adding aspects, as citizens are outspoken and have no issue with protesting to garner the government's attention. Civil organisations/citizens are involved with several government sectors, including political, social, safety and security, and the economy. They are very focused on all socioeconomic aspects that directly influence their lives. Neethling (2014:44) describes *socioeconomic conditions as an indicator attempt to measure the satisfaction or dissatisfaction with a country's government's socioeconomic policies by citizens. Relevant socio-economic factors vary from country to country and include, among others, aspects ranging from infant mortality and medical care provision to interest rates.*

The above understanding of SA's society needs further analysis and investigation. Schwella (2017:232-234) observed that *according to the UNDP (2021), the HDI is a summary measure for assessing long-term progress in three basic dimensions of human development, namely: A long and healthy life; Access to knowledge; A decent standard of living*. Considering the above background regarding society and its direction of government services, a table was created to reflect these aspects for SA. The table shows that SA is progressing well but several violent protests ('Fees must Fall', service protests, and 2021 protest and looting, which will be analysed later in this section) have influenced the gradings and indexes internationally over the past decades.

Table 13: SA HDI expectancy at birth, schooling and PPP: 1995 to 2021

Year	1995	2000	2005	2010	2012	2014	2016	2018	2020	2021
HDI	0.661	0.633	0.632	0.675	0.696	0.712	0.719	0.726	0.727	0.713
Life expectancy at birth	62.3	54.8	54.0	58.9	61.8	63.4	64.7	65.7	65.3	62.3
Expected years of Schooling	12.9	13.1	13.3	13.4	13.5	14	14	13.5	13.6	13.6
Mean years of Schooling	8.3	7.3	8.9	9.7	9.9	10.1	10.2	10.8	11.4	11.4
Gross National Income (GNI) per Capita (PPP/R)	10,277	10,823	12,299	13,335	13,602	13,701	13,545	13,491	12,450	12,948

Source: Researcher's construct (Data adapted from UNDP, 2022)

The UNDP (2021) report shows that SA's HDI value was 0.713 in 1995, which increased every year but declined by 0.014% due to the July 2021 incidents and the Covid-19 pandemic. This places SA in the high-human-development category, at 109 out of 187 countries and territories. Between 1995 and 2021, SA's HDI value increased from 0.661 to 0.713, an increase of ±10%, or an average annual increase of about 0.3%. In 2011's HDI, SA was ranked 123 out of 187 countries (UNDP, 2013). Thus, SA has enhanced its ranking by 14 positions in the last decade (with the table above showing individual results for each aspect). In summary, an analysis of the data showed:

- Life expectancy at birth decreased by 3.5 years during the HIV/Aids pandemic from 2000 to 2010. However, it had increased to 63.8 in 2018 and declined slightly during the pandemic;
- Mean years of schooling increased by 3.1 years;
- Expected years of schooling increased by 0.7 years; and
- GNI per capita increased by about 14% (2018) and decreased from 2019-2021 by 1.5%.

SA, compared with other countries with rapidly emerging economies, specifically with the BRICS countries, the BRICS subgroup IBSA and the CIVETS countries, can be presented in the table below. Compared to BRICS and CIVET countries, SA is rated in fourth place. Compared to IBSA countries, SA is rated in second place and below the world average. These results show that SA is still lagging behind most of their peers in the emerging economy group.

Table 14: BRICS, CIVET AND IBSA Countries HDI: 2020 to 2021

BRICS, CIVET AND IBSA COUNTRIES			
	COUNTRY	YEARS	
		2020	2021
BRICS	Brazil	0.758	0.754
	China	0.764	0.768
	India	0.642	0.633
	Russian Federation	0.830	0.822
	SA	0.727	0.713
CIVET	Colombia	0.756	0.752
	Indonesia	0.709	0.705
	Vietnam	0.710	0.703

BRICS, CIVET AND IBSA COUNTRIES			
	COUNTRY	YEARS	
		2020	2021
	Egypt	0.734	0.731
	Turkey	0.833	0.838
IBSA	India	0.642	0.633
	Brazil	0.758	0.754
	World average	0.735	0.732

Source: Researcher's construct (Data adapted from UNDP, 2022)

The UN DHI provides the necessary birdseye view of the progress made by countries over a long period of development. Schwella (2017:233-234) states these results indicate that *this trend is probably strongly linked to policy and governance failures related to health-service policy and governance in SA, where ideological thinking and action trumped evidence-based public value and learning governance. These aspects of governance represent the potentially disastrous effects of governance going wrong through bad public and governance leadership.* The Expert Panel (2022:51) confirms Schwella's views, relating them to the July 2021 protests in KZN and Gauteng: *most importantly, government, at all levels, must seriously attend to the country's socioeconomic challenges. We will fail in our duty if we fail to express the profound frustration from the civil society, business, and security sector delegations we met that the government is not paying sufficient attention to this matter. The internal contradictions within the ANC are impacting negatively on governance matters and need to be resolved.* Furthermore, the ISS (2022) indicates that internal contradictions within the ANC also affected the country's socioeconomic issues. *The ANC's failure to manage elite contestation in its ranks since 2007 has seen tensions spilling out, often as 'service delivery protests. Former president Jacob Zuma controlled this infighting largely through patronage and repression. The sharp rise in protests from the end of 2017 suggests that President Cyril Ramaphosa does not seek nor have the same autocratic power as his predecessor. Instead, he is trying to manage internal party disputes within the constitutional framework by rebuilding institutions weakened through state capture* (ISS, 2022:1). These protests had a severe impact on SA's economy, with clear evidence of the ANC's misuse of the country's poor.

The 2021 South African Reconciliation Barometer (SARB), a nationally representative public opinion survey conducted regularly by the IJR, aims to provide a measure of several aspects of public opinion. The table below shows the opinions of the public regarding their trust in individuals, institutions, and political parties. The public trust in some government institutions is alarming, specifically Parliament, justice system institutions, political parties, and religious leaders.

Table 15: Data from SARB Survey 2021 Report

SA Reconciliation Barometer Survey: 2021 Report	
Institutions, Individuals and Political Parties	2021:% Confidence
SABC	52
SARS	45
Hawks	43
President	42

SA Reconciliation Barometer Survey: 2021 Report	
Institutions, Individuals and Political Parties	2021:% Confidence
Religious Leaders	40
Constitutional Court	38
Big Business	37
SAPS	37
Public Protector	37
Parliament	37
NPA	36
ANC	36
Legal System	35
National Government	34
Provincial Government	33
Local Government	31
DA	31
Deputy President	30
EFF	24

Source: Adapted from SARB (2021 Report)

Shockingly, Table 15 shows that SA does not trust Parliament, NPA or the justice system, yet these institutions must be trusted in a democracy. The public's opinions regarding poverty are based on the fact that their lives never seem to improve, which can largely be attributed to the government's poor service delivery. The Afrobarometer survey (2021) results indicate SA citizens' essential issues over the past three years (Table 16). Some of these aspects were identified by former President Mandela in his speech to the WEF in Switzerland in 1992 (New York Times, 2013:1) (as described by Mr Mboweni): *That message was about how the ANC intended to achieve social justice for the majority black people: decent housing, health care, decent education, public transport, access to clean water, sanitation and access to what I called 'the means of production,' that is, the creation of a black business class. That is all. No capitulation.* Additionally, former President Mandela proposed an open and free economy for SA. Whilst the ANC stuck to this plan from 1994 to 2008, under former President Zuma, the wheels came off.

Table 16: Most important problems identified in SA: 2021

Most Important Problems Identified by Survey in SA: 2021				
YEAR	2011	2015	2018	2021
Unemployment	70%	71%	62%	60%
Crime and security	29%	27%	29%	29%
Housing	30%	27%	24%	26%
Education	14%	22%	18%	24%
Corruption	24%	24%	19%	20%

Source: Researcher's construct

This table is a reflection of Tables 5 and 6 in Chapter Two of this dissertation. The tables indicated people's biggest fears (in Africa and the rest of the world). Based on the table below, the ANC has attempted to provide for these fears/needs (Cronje, 2017:40-41). An important issue that is mentioned in these tables is unemployment, which was at 23.9% in 2012 (StatsSA, 2012a:56). It went up to **35.3%** in the fourth quarter of 2022, with the most concerning figure relating to the 15-

34 age group in SA, which some analysts view as a ticking time bomb (IOL, 2021:1; StatsSA, 2022). Unemployment further increased due to Covid-19, which caused many businesses to close.

Table 17: Basic needs of society that government complied with

Basic Needs Complied with by Government			
Years	1995/6	2016	2021/22
Unemployment	29.89%	26.54%	35.3%
Water	7.2 mil with tape water	14.3 mil with tape water	89.4%
Electricity	42% without	10% without (2016)	84.39%
Housing Formal	64% with formal housing	78.1% with formal housing (2015)	83.6%
Housing Informal	16% with informal housing	14.1% with informal housing	11.7%
Education Grade 12	201 284 passing grade 12	321 221 passing grade 12	537 687 passing grade 12
Education Higher	575 412 enrolled for a degree	969 154 enrolled for a degree	1 093 353 enrolled for a degree

Source: Researcher's construct

Unemployment is also influenced by the country's poor economic development. The UN (2021) and IMF (2022) reports indicate that SA has more severe problems because of its workforce's skills and education levels, which indicates high political risk and social instability. At most, they face challenges posed by *African voters [who]) demand more than historical mobilisation as justification for their vote, particularly in urban areas where social media is experiencing massive growth* (Cilliers, 2012:2, in Neethling, 2014).

The 2021 and 2022 surveys by Afrobarometer, StatsSA and SARB were conducted during a challenging period in SA history, highlighted by violence, protests and the lockdown due to Covid-19. Politically, the dominant ANC is experiencing a decline in voter support, and the Zondo Commission implicated the elite in state capture, corruption, and influencing people to take part in these wrongdoings. Former President Zuma was arrested for not complying with a Constitutional court ruling. Despite being remarkably dynamic and fast-moving, the country's opposition parties struggled to use this opportunity to win some support for their parties.

Socially, the barometers showed that there is considerable mistrust in society. SA society is plagued by high levels of crime, not receiving the basics to make a living, the high unemployment rate, and the impact of Covid-19. The government tried to soften the pandemic's impact by giving state grants to the poor but not before helping itself to a large portion of the funds. These aspects hamper development and exacerbate social problems experienced by the public, proving SA institutions' vulnerability during a crisis.

In summary, SA is described as an active, often activist (Schwella, 2017) society that enforces itself through protests and media attention, creating a problem for the current regime. Its citizens are still divided by inequality, and a high percentage of people live in poverty and are unemployed, especially youths between the ages of 15 and 35. The government has tried to overcome these

issues by providing social grants, free housing, electricity, and water (a temporary solution). As a more permanent solution, the government will need to ensure investments and job opportunities.

5.2.8.3 Security

Chapters One and Two of this study defined national security as*…the first and most important government obligation. It involves the safety and security of the country and its citizens. It is a matter of guarding national values and interests against internal and external dangers – threats that can potentially undermine the security of the state, society, and citizens. It must include not just freedom from undue fear of attack against their person, communities, or sources of their prosperity and sovereignty but also the preservation of the political, economic, and social values – respect for the rule of law, democracy, human rights, a market economy, and the environment – which is central to the quality of life in a modern state* (IWGNS, 2013:3).

This section of the chapter will focus on **Safety and Security** in the SA landscape and its impact on the economy and people. Neethling (2014), Fouche (2003), ISS (2022) and StatsSA (2021) all described SA's crime problems, which have improved over the past decades, as a very severe threat to the socioeconomic development of SA. Neethling (2014) describes safety and security as law and order. Furthermore, according to Fouche (2003:36), *law entails an assessment of the strength and impartiality of the legal system, whereas order relates to an assessment of the widespread observance of the law of a country*.

The ISS (2022) analysed violent crime and protest action in SA as a threat and risk to the political stability in the country. These aspects cannot be linked to unemployment and poverty (traditional research) only but some of the ANC factions' political elites are involved. The ruling elite's connection to these crimes also placed police and intelligence services in a complicated position. Protests negatively impact foreign and local investors (Neethling, 2016). The author states that according to the Transparency International Corruption Index (2014), SA was rated 48th out of 140 countries in 2013, a rating which fell to 70th out of 180 countries more recently. Currently, researchers, academia and journalists call SA the protest capital of the world (Mail & Guardian, 2010).

Neethling (2016:52) states that *social risk in the form of **service delivery protests** has increased markedly, and this phenomenon remains a factor of the most significant concern in any consideration of forces and events that could negatively influence investors' confidence*. The Municipal IQ, an independent local-government-monitoring agency, confirms these concerns on their website (Municipal IQ, 2022). It indicates that the number of violent protests against the local government has risen over the years, as these municipalities cannot render good services to their

communities. These protests and their resulting violence create fear in the public environment and also create a high level of fear and distrust in the police and law enforcement (StatsSA, 2014).

A prominent protest was Lonmin's **Marikana Mine** tragedy, which occurred on 16 August 2012 in the Rustenburg area of the Northwest Province. This protest drew international attention to the SA political environment due to several violent incidents that transpired between Lonmin security, the National Union of Mineworkers (NUM), the striking Lonmin workers and SAPS. The majority of the 40 people killed by the SAPS were striking workers, with roughly 80 injured (however, the exact number of injured workers is unknown). Such incidents negatively impact the economy and discredit SA internationally.

Furthermore, findings from recent surveys and research indicated that between 2000 and 2008, **xenophobic attacks (and murders)** have become another serious political issue in the SA context. Neethling (2013), SARB (2021) and Afrobarometer (2021) indicate that xenophobia and violence against immigrants have increased in recent years, with a marked escalation occurring from late 2000 to 2008 (Human Rights Watch 2021). Furthermore, in this period, *67 people died, of which 21 were later declared SA citizens*. From 2008 to 2022, attacks took place throughout SA, and an anti-immigrant movement and operation were formed, namely 'Operation Dudula and Dudula'. (Daily Maverick, 07 Jul 2022). In several studies, it was found that the number of immigrants in SA has risen over the past two decades, increasing from 2 to 4 million people between 2010 and 2017. Secondly, the public is growing increasingly hostile towards immigrant communities, according to the Pew Research Centre poll (2019): *62% of SA citizens view immigrants as a burden, who take their jobs and social benefits*; in addition, *61% of SA citizens thought that immigrants are responsible for more crimes than any other groups; The immigrant communities grew the proportion of SA's total population from 2.8% in 2005 to 7% in 2019; The widespread xenophobia in the country has not deterred the immigrants from coming to SA.* This statical data and information show that SA was the largest recipient of immigrants on the African continent in 2019, despite the general population's xenophobia. Unfortunately, these attacks can become a severe threat to security on an international level; for example, Nigeria's response to the attacks on its citizens (Africanews, 2019).

In addition, **anti-state opposition** should be understood as not including opposition political parties (Neethling 2013) in the country or territory. This area or threat comes from groups or individuals who want to take over or disrupt a country or territory through revolution, revolts, and terror. According to ISS (2017), since 1990 the potential of revolution or revolts against the government has decreased; however, specific incidents regarding extremism in SA emerged, and these types of threats are possible in the future. No threatening neighbouring state or superpower in the

Southern Africa region can influence any state's stability (Neethling, 2012). The SA government has embarked on a political drive to enhance their role and image with the rest of Africa, specifically with the Southern African Development Community (SADC) countries. Former President Mbeki attended to these aspects with his visits to other African countries. His activities brought SA into the international environment with positive results for the economic development of SA (Neethling, 2012).

This section will focus on the aspects that hamper SA's economy and development the most. As mentioned, SA is branded the 'protest capital of the world'. One such example is the 2016 student protest, '**Fees must Fall'** (Rand Daily Mail, 31 October 2016) which interrupted universities and resulted in millions of rands of damage, with police and the government's security cluster struggling to contain the situation. This protest revealed just how much influence certain people have in civil society, as elements outside the universities influenced the students' campaign. This protest severely damaged law enforcement agencies' image. The July 2021 violent protests and looting (ISS, 2022) are a further example of communities being influenced by individuals with opposing views. They misused the arrest of former president Zuma as the reason to protest, and soon after widespread looting began in KZN and Gauteng. The public tried to secure their homes but business owners were helpless against the mobs, suffering millions of rands of damages and theft, and more than 300 people lost their lives. Unfortunately, this protest may only be a precursor. The Expert Panel (2021:4) reported that: *The question, many argue, is not if and whether more unrest and violence will occur, but when it will occur*. This situation puts everybody in a negative mindset, and foreign investors will think twice about investing in a country like SA. The Expert Panel (2021:4) report further states *This bleak prospect can be avoided if there is a clear understanding of what happened, and better planning and coordination leading to a coherent approach in dealing with the mounting social and political challenges that our society is facing*. Although more than a year has passed since the chaos of July 2021, a panel was created and several possible coordinators were arrested, they still need to be charged in a court of law and the government is yet to clarify exactly what happened and who coordinated or instigated this protest. Opposition parties and analysts suggest that several instigators were recalcitrant members of factions within the ruling party (ISS, 2022). This incident, and all others mentioned, have been earmarked as reasons for SA's economic/development shortfall and international down gradings.

The Sunday Times (2022:13-14), as well as Shaw and Rademeyer (2022), wrote about **organised crime** in SA, which threatens the country's democratic institutions, economy, and citizens. The article highlighted the shocking murder statistics in SA - 40 murders per 100 000 people, which is higher than Mexico with all its drug cartels. The crimes that form part of these organised crime syndicates were divided into three specific categories:

- **Selling the illicit:** older and established markets for drugs, illegal firearms, human trafficking, wildlife smuggling, fishing, and environmental crime;
- **They deal in violence**: Extortion, kidnapping for ransom, organised robbery and violence, which includes murder-for-hire; and
- **Preying on critical services**: Attacks on critical infrastructure, organised corruption, cybercrime, economic and financial crimes, health sector crime, crimes in mass public transport (including minibuses and buses), and illegal mining.

These crimes occur daily, and the police struggle to handle these criminal investigations. This influences everyone in SA, gives our country a bad image and does real harm to the tourist industry which is still trying to recover after the Covid-19 pandemic. Shaw and Rademeyer (2022) believe all these crimes are linked to the underground economy and activities.

Further issues include drive-past tavern shootings and a whistle-blower from the Department of Health in Gauteng being assassinated, creating an impression that the SAPS does not have control over crime. The Minister of Police gave a feedback session to Parliament in October 2022, reconfirming these threats in SA (Daily Maverick, 2022). He confirmed that the police could not comply with most of the objectives in their strategic plan for the last financial year because of poor work conditions for officers and the high number of skilled officers leaving the force. In addition, budget constraints prevented recruits with the necessary qualifications and skills from being hired. These feedback reports and articles confirm that SA is experiencing a severe violent crime wave that needs to be neutralised as soon as possible. Fortunately, October 2022's Medium Budget Policy Statement by the Minister of Finance brought some good news, specifically for the SAPS, which received an additional R3.1 billion to recruit more law enforcement officers (SA, 2022).

Energy and Water Security is becoming a huge political risk and threat to SA and could bring the country to its knees. News24, Patrick (2022) wrote an article stating that the current water situation in Gauteng's biggest metros is becoming a crisis; *Prof. Turton of the Free State University, a water expert and researcher, 'is concerned that officials could be downplaying the issue. Turton states 'What we are seeing is a systemic failure as different systems are starting to fail. Water and energy and sewage are all in state of [failure] across the country. Furthermore, It is quite alarming when government officials choose to shift blame or trivialise the problem. Dr Adam, an environmental activist and manager at WaterCAN states: There is a national collapse of the water system. The government says we do not have a crisis. The government says water shedding is isolated. This is not true.* The author added that the water crisis was due to *poor planning, failing infrastructure, underspending of budget, corruption created by poor governance. The author added that the country will not have enough water supply to meet the demand in 2025.* This crisis is beginning to

sound similar to the issues faced by ESKOM in 2007, which were ignored. SA's energy crisis (load shedding) has a severe impact on the economy (BusinessTech, 2022). The WB (ESI Africa, 2022:1) indicates that SA needs to change their energy fleet to more environment-friendly technologies, which will not only overcome its electricity shortfall but also positively influence its economy, which needs many investments to grow. Economic growth will decrease unemployment and provide financing for the infrastructure.

This section must mention **Food Security** due to its future impact; additionally, SA's water and energy crisis could dramatically increase this problem. Nhamo (2022), a research manager at the Water Research Commission, argues that *to meet future world food and nutritional demands. Food production must increase by approximately 70% by 2050* worldwide to sustain the demand. The author argues that countries' entire food systems must change toward sustainability because essential resources such as water, energy and land are depleting and degrading. *The challenges are compounded by climatic and environmental changes induced by unsustainable food systems*. This will be challenging in the SA context as two prominent aspects hamper the necessary changes that must be made, namely the ANC's questionable land reform and water/electricity problems that are already an issue. The country's agriculture sector is currently providing necessary food levels but for how long that will be the case, with the two aspects mentioned above, is very uncertain.

In summary, the security environment in SA is a huge problem from a crime perspective (violent protests, looting, corruption, xenophobia, and organised crime), including a few other essential aspects that influence the economy and severe infrastructure losses. Crime must be controlled and handled by government law enforcement agencies, of which the SAPS is the most important institution. The energy and water security areas are also critical aspects which need urgent attention from the government. These two securities will severely influence the country's food products and it's needs as identified for 2050. However, currently, food production is high, and SA exports many products to the rest of the world. Finally, and importantly, security issues influence the next most crucial aspect in political risk evaluation, namely the economy.

5.2.8.4 Economy

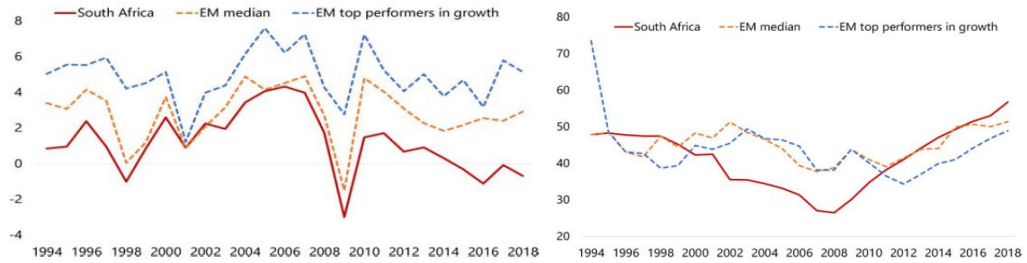
On Investopedia's website, Kenton (2022) states that *an economy is a complex system of inter-related production, consumption, and exchange activities that ultimately determines how resources are allocated among all the participants. The production, consumption, and distribution of goods and services combine to fulfil the needs of those living and operating within the economy.* What is happening in SA's economy is interesting because, as the New York Times (2012) reports, former president Mandela changed the ANC's economic policy before presenting it to the WEF in Davos.

Sorkin of the New York Times (2013) states that *it happened in January 1992 during a trip to Davos, Switzerland, for the annual meeting of the WEF. Mr Mandela was persuaded to support an economic framework for SA based on capitalism and globalisation after a series of conversations with other world leaders. Mr Mboweni: We discussed this at some length and decided that the content was inappropriate for a Davos audience; So, I drafted a short message for the audience. He added that message was about how the ANC intended to achieve social justice for the majority of black people: decent housing, health care, decent education, public transport, access to clean water, sanitation, and access to what I called 'the means of production', that is, the creation of a black business class. That is all. No capitulation. However, as the five-day conference wore on, Mr Mandela soon decided he needed to reconsider his long-held views: Madiba then had some exciting meetings with the leaders of the Communist Parties of China and Vietnam, Mr Mboweni wrote, using Mr Mandela's clan name. They told him frankly: 'We are striving to privatise state enterprises and invite private enterprise into our economies. We are Communist Party governments, and you are a national liberation movement leader. Why are you talking about nationalisation?; It was those decisive moments which made him think about the need for our movement to rethink the issue seriously. Mr Mboweni added that Mr Mandela's push toward free markets opened up his country to become the fastest growing in Africa and eventually brought in billions of dollars of investment from large companies outside the country. The statistical data showed this growth during the period 1994 to 2008. The ANC government provided those services as mentioned by Mr Mboweni: decent housing, health care, decent education, public transport, access to clean water, sanitation, and a black business class.*

Nonetheless, Cronje (2020) states that *these circumstances, together with the pragmatism of GEAR, saw SA begin to make economic progress. The economic growth rate rose to about 3% between 1994 and 2003 before lifting to an average of over 5% between 2004 and 2007 - the first time the economy had averaged growth at that rate for four consecutive years since 1970.*

The ANC's decisions saw SA's first budget surplus in 50 years, and the government could also limit debt levels. Although tough decisions had to be made, they led to a change in economic policy, thus creating a Black middle class in SA that, today, is bigger than the White middle class. Unfortunately, under the Zuma administration, economic policies were hijacked and the economy was damaged through unrelenting and unashamed corruption. This was exacerbated by poor economic policies which provided individuals and groups with the opportunity to be involved in state capture and labour union domination, thus slipping over into violent protests and strikes. Furthermore, when the 2009 financial crisis hit, the left-wing of the ANC pursued a revolution, chasing many potential investors out of SA. Thereafter, the energy security crisis began (2007-2011) creating more economic problems for the country. Alongside economic deterioration came

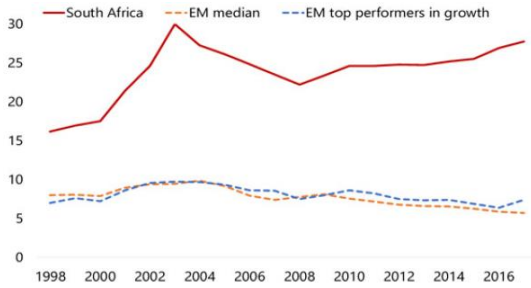
unemployment, and service protests became the norm. To illustrate these trends, the figure below shows the GDP growth of SA in comparison to other emerging market countries from 1994 to 2007, with the severe drop in 2009 due to the world economic crisis, and then the bounce back in 2011. From there onwards, the economy has deteriorated to growth rates of below 1%. Furthermore, it can be seen that SA has performed below its peers for decades.



Source: Reproduced from IMF (2020)

Figure 25: Real GDP per capita growth and GDP compared with other emerging markets

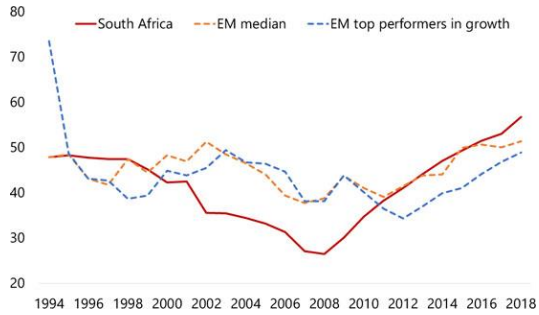
SA has clearly fallen behind other emerging markets' GDP terms and rankings. In October 2022, the Minister of Finance (SA, 2022) indicated that in the short- to medium-term: *Domestically, the robust pace of economic recovery in early 2022 was derailed by floods in various parts of the country, particularly KwaZulu-Natal and the Eastern Cape; industrial action in key sectors, and widespread power cuts. We now expect real GDP growth of 1.9% in 2022, compared with an estimated 2.1% in February. Over the next three years, the economy is expected to grow at an average of 1.6%. This level of growth is too low to support our developmental goals. Accordingly, we must take action to put our economy on a higher growth trajectory.*



Source: Reproduced from IMF (2020)

Figure 26: Unemployment in SA: 1998 to 2016

From the figure above, it is clear that poor economic results impact employment and job creation in the country; with unemployment at its highest under the new democratic SA. The unemployment results in the fourth quarter of 2022 (StatsSA, 2022) show a staggering 35.3%. These numbers should be alarming because over 50% of those people include the youth between the ages of 15 and 35; many of whom are not well-educated and do not have specific skills. Unemployment is a ticking time bomb and puts SA's economy and development under a severe threat.



Source: Reproduce from IMF (2020)

Figure 27: SA's gross debt against emerging markets' debt

SA's poor performance in the global environment also reflects in the gross debt against its peers, as shown in the figure above. Evermore, the government's spending increases, and they need to borrow more money to pay for their spending due to higher personnel costs, poor supply chain costs, poor management, poor economic and labour policies, and corruption in government institutions.

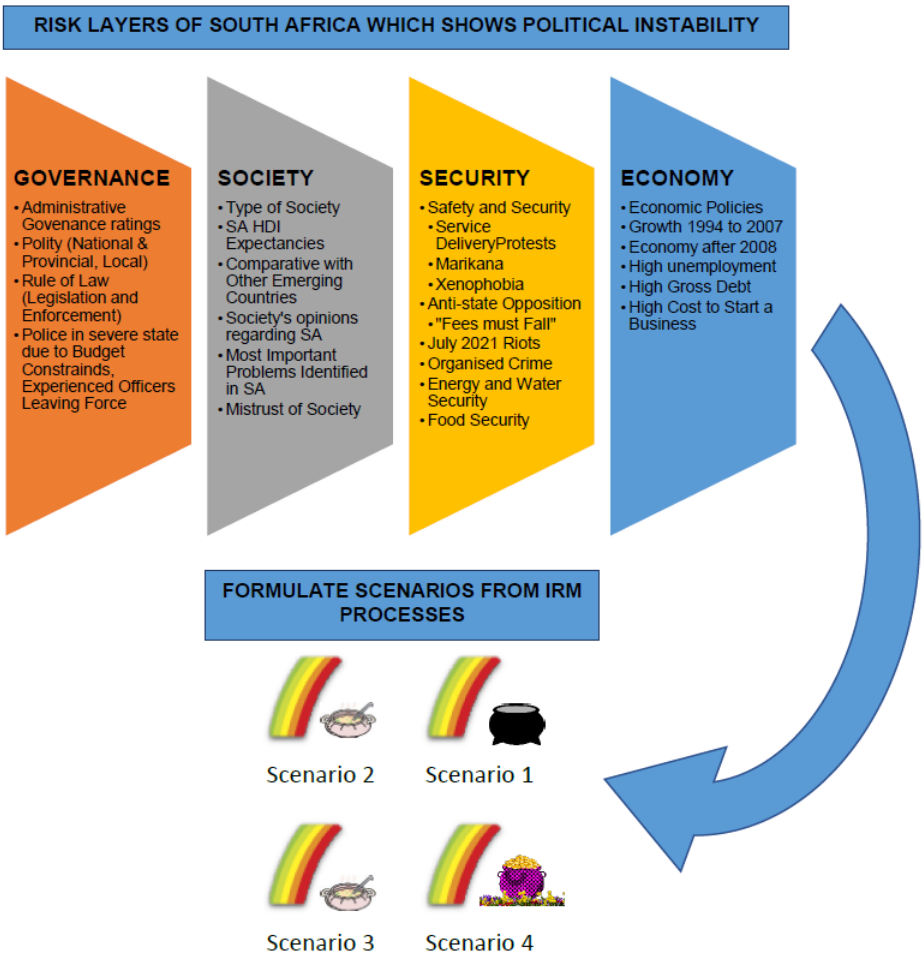
The Minister of Finance (2022) also identified the following aspects which influence the economic growth of the country from an international and domestic perspective: *Globally, these include rising inflation, tightening financial conditions and the ongoing effect of Covid-19, including the more stringent lockdowns in China and their impact on global demand and supply chains. These were made worse by the outbreak of the Russia-Ukraine conflict*. [Domestically] *Several long-standing structural impediments continue to hamper growth. These include unreliable electricity supply, costly and inefficient ports and rail networks, crime and corruption, weak state capacity, and high market concentration levels and entry barriers suppress small business emergence and growth.* By addressing these threats, risks and vulnerabilities, the government has shown that it is focused on these problem areas, which has been well received by society, specifically analysts and academics.

SA also needs to address the high cost of starting a business, as entrepreneurship is key to driving up the economy and reducing unemployment. In his Medium Budget Policy Statement, the Minister of Finance (2022) stated *We seek to reverse these trends by tackling impediments to investment*. In the private sector, policy uncertainty, constraints to the ease of doing business, and the high cost of doing business are often cited as critical constraints to investment. The IMF (2021) noted that *SA's cyclical recovery in 2021 has been relatively strong, with estimates of a 4.6% GDP rebound after the economy contracted by -6.4% in 2020. It said that the recovery was also supported by external factors, such as favourable commodity prices and benign financial conditions, which are likely temporary. However, it warned that the rebound had not decreased the unemployment rate amid deteriorating confidence, exacerbated by the July 2021 social unrest episode, anaemic private-sector investment, and weak credit extension. The IFM Staff, therefore, projects a lacklustre*

medium-term outlook, with growth averaging 1.4% per annum, inflation returning to the midpoint of the 3%–6% target range, and the external current account reverting to its structural deficit.

These remarks by the IFM summarise SA's economy well - as under severe pressure from global and domestic environments. The analysis of the above four variances showed that SA is a volatile state, constantly disrupted by strikes and protests, which often turn into violent action (ISS, 2022). These aspects hamper economic development and investment from foreign entities. The four variances influence each other and must not be viewed in isolation. Therefore, the poor governance reflected in the analysis applies to all three levels of government (national, provincial and local). Polity in SA creates most of the poor governance and violent protest action; with the current regime prolonging legislation adjustments and implementation. These aspects create an economic and security threat and risk to SA (terrorism, international crime and lack of investments). Analysts view SA's severe inequality, unemployment, poor education and skills as serious impediments which must urgently be corrected by the government (perhaps, with universities' assistance).

The security variance analysis showed that the critical fields of energy, water and food security need serious attention from the government and specialised institutions to ensure that SA does not deteriorate even further. Not only is electricity near collapse but water supplies are under pressure, which both threaten future food security. These aspects severely impact the economy, which carries a significant burden due to poor policies and lack of reform by the ANC. This hampers growth and opportunity for skilled and unskilled citizens alike. This background forms the basis for formulating the scenarios in the next section. The analyses of the four variances in this section can be captured in a figure which shows the conceptualised framework for risk layers, as seen below.



Source: Researcher's construct

Figure 28: Risk layers of SA which show political instability and Formulated scenarios

5.3 Constructed Plausible Scenarios for the South African Context

The above information and analyses provided the necessary information for the IRM process to formulate scenarios which can better advise the policy-maker or client. This research drafts four scenarios, named the rainbow pot scenarios (as seen in Figure 28 above). Therefore, according to the matrix in Figure 24 (Section 5.2.7), Scenario 1 describes a country shaped by high levels of political risk in an unstable political environment. Scenario 2 describes a country shaped by high levels of political risk in an environment of low instability. Scenario 3 describes a country shaped by low political risks in an unstable political environment. Finally, scenario 4 describes a society shaped by low levels of political risk in a stable political environment. Thus, the research will now determine (through IRM processes) the necessary rainbow pot scenarios which are influenced by the two axes of stability and instability and political risk (high and low) in SA (Figure 24).

The metaphorical rainbow comes from the nation concept created in the first decade of the new democratic SA during former President Mandela's rule. The three-legged pot is known to most SA citizens because they provide food for their families in it.

5.3.1 Scenario 1: Worst case scenario - Empty pot: (20% probability)

This scenario is plotted in Figure 24 as the 'Worst Case' category with high political risk and instability facing SA. The scenario is based on the risk layers framework depicted in Figure 29, which analyses and reflects this futuristic scenario probability in SA. In this scenario, President Ramaphosa is not re-elected, and the more left flank of the ANC dominates the elections during the ANC's 55th elective conference. The dominant ANC regime does not obtain a majority in the 2024 elections and needs to form a coalition government. They decide to opt for a coalition with the EFF. The EFF puts pressure on the ANC and claims some significant cabinet positions in return for their coalition arrangement. Moreover, the EFF enforces its political views onto the ruling coalition partner and the nationalising of banking, mining, and land is forced onto SA's political environment. Governance deteriorates, and institutions cannot provide quality services. The energy and water security sectors fail, and only emergency maintenance is done. Society is frustrated with the government due to insufficient services, unemployment, security, and safety issues. The unemployment results break all previous records. Furthermore, out of frustration, citizens start to protest more violently; people lose their lives and infrastructure is destroyed. Weak global growth and the absence of any local economic reform agenda causes SA's growth potential to plunge toward zero. A sovereign credit rating downgrade spiral ensues, and there is an increased probability of an IMF or WB bailout.

5.3.2 Scenario 2: Base case scenario - Half-empty pot: 'Muddle Through' (60% probability)

This scenario is plotted in Figure 24 above in the 'Muddle Through' category with high political risk and stability facing SA. The scenario is based on the risk layers framework depicted in Figure 29, which analyses and reflects this futuristic scenario probability in SA. In this scenario, President Ramaphosa is re-elected, and the political situation has not changed. The NEC is still divided evenly between left flank members and the so-called reformers. The ANC regime wins the 2024 elections with a majority of 50%. Moreover, the current poor governance continues; there is prolonged economic growth, the poor of SA endure hardship, and unemployment rises. The biggest threat to the SA landscape is not only electricity but water as well. These two securities hamper any growth and investments in SA. The disgruntled society becomes increasingly frustrated with the government, and significant violent protests occur more frequently. Some opportunities are taken by the government for a more successful SA. The government makes policy changes regarding the

economy and labour which ensure a speedy recovery of the economy. The government embarks on a serious recruitment drive to replace most cadre deployments, enhancing governance by at least 60%, if not more. Realistically, it is uncertain if the ANC has the necessary will to do so.

Therefore, **Scenario 2: Sluggish domestic growth,** includes i) global growth at 0.5 percentage points lower than forecast; ii) oil prices staying elevated because of the Ukraine/Russian war; iii) interest rates increase to offset inflationary pressures from a weaker rand; iv) SA's GDP grows by 1.4 to 1.6% in 2023-24; v) the gross debt-to-GDP ratio climbs to 80% by 2026-27; and vi) primary budget deficit peaks at 2% in 2023-24 due to high costs to ensure energy and water security.

5.3.3 Scenario 3: Base case scenario - Half full pot: 'Rebound' (15% probability)

This scenario is plotted in Figure 24 above in the 'Rebound' category with low political risk and instability facing SA. The scenario is based on the risk layers framework depicted in Figure 29, which analyses and reflects this futuristic scenario probability in SA. In this scenario, the ANC does not obtain the majority 50% during the 2024 election, and the ANC enters into a coalition with some of the smaller political parties, excluding the EFF and DA. The coalition works well, and some instabilities are experienced due to the left flank of the ANC, which is not happy with the coalition arrangements. The newly formed coalition made some economic and labour policy changes. These steps send the correct message to foreign investors. The land reform issues are resolved, and there is more clarity regarding land reform and foreign property rights. The economy does not recover quickly but gains 2% and levels out at 3.2% to 3.5% of GDP. The government arranges to recruit new executives with the proper education and skills to fill senior posts in the public sector. This elevates the standards of service delivery in the government environment. Universities are requested to assist with the training and coaching of the executive levels in the public domain.

Therefore, **Scenario 3: Prolonged domestic growth** involves i) global growth at 0.5 percentage points higher than forecast; ii) oil prices are lower because Ukraine/Russian started peace talks; iii) interest rates are lower due to a stronger rand; and iv) debt is stabilised at 58% of GDP in 2027-28.

5.3.4 Scenario 4: Best case scenario - Pot of gold: 'Reflation' (5% probability)

This scenario is plotted in Figure 24 above in the 'Reflation' category with low political risk and stability facing SA. The scenario is based on the risk layers framework depicted in Figure 29, which analyses and reflects this futuristic scenario probability in SA. In this scenario, the ANC does not obtain the majority 50% during the 2024 election, and the opposition parties gain control of the government in a coalition between the DA and smaller parties. The new regime starts cleaning up poor governance. The government calls on the private sector to support a new development plan

to counter unemployment and poverty. Universities are requested to support research projects to enhance the poorly educated and skills base of the unemployed in the country. Budget allocations for law enforcement agencies are revisited to ensure a clamp down on high crime rates. Fast economic reforms initiated by the coalition government ensure the economy's gradual recovery due to foreign investments. This economic growth, supported by solid global economic growth, lifts SA's growth potential above 3% in the short-term. Economic growth enables the country's credit rating to move closer to investment grade in the longer-term. The embattled SOEs (ESKOM, Water boards, DENEL, Landbank and others) receive help from the private sector, and some are even privatised to relieve the fiscal framework.

Therefore, **Scenario 4: More robust domestic growth,** includes i) GDP expansion that reaches 3.2% in 2025-26; ii) state achieves a primary surplus of 0.5% by 2027-28; and iii) debt is stabilised at 55.4% of GDP in 2027-28.

This described scenarios would direct SA to any one of these outcomes. For more information, see Schwella (2017:226-318); IMF Country Report SA (2006-2020); WEF (2022); World Risk Report, SAPS. 2014: 2(1); StatsSA (2021); IIAG (2022); TICI (2022); UN System Task Team (2012), and WB (2018).

5.4 Conclusion

Chapter Five aims to formulate futuristic scenarios that can provide policy-makers and clients with a more informative intelligence product that can direct policy decisions. The principles as described in Chapters Two to Four were followed. Firstly, in this chapter, the concepts of stability and instability were defined and secondly, the chapter investigated why SA is so easily influenced and destabilised, which influences its economic and development path. It was identified that SA falls in a category of countries in Africa that show good socioeconomic and development growth with an absence of instability aspects influencing their growth. That proves that SA needs to be stabilised to ensure growth.

The chapter further developed a framework that can provide the necessary data which can be analysed to determine why SA is unstable. Other scientific tools were combined with this framework, and scenario planning and building tools formed part of the methodology used in the chapter. Nevertheless, from this process, it was possible to draft four scenarios regarding SA's future. These processes showed that Johnson (2009:52) is correct in stating that intelligence borrows methodology successfully from other science fields.

This chapter combined the scenario methodology of Schwartz (1996), Cronje (2010, 2016 and 2020) and Eurasia Group (2008) to build a scenario plan and framework to analyse SA's instability. It provided the necessary structure to determine SA's governance, society, security and economy and gave an overview view of the variances influencing the SA environment. The Eurasia Group framework (matrix) was used to analyse the SA political environment from the following four variances: governance, society, security and economy. The four variances were defined to understand these areas from a political science perspective, which provided a balanced approach to each variance. The focus was not only on destabilised phenomena but also on the government's success during a specific period from 1994 to 2022. The analyses showed that there are defined threats, risks, vulnerabilities and opportunities in the SA political risk environment that must be resolved to ensure growth.

The governance environment was influenced due to poor service delivery, prolonged legislative and policy formulation processes, corruption and a polity which all strived to control and lead the country, without focusing on the essential aspects of society. ISS (2022:1) found, through research, that the ruling party (ANC) elite and members are involved in the many protests that are taking place in SA's environment, which is a severe threat to the stability of the country and will influence the future coalition formed on all levels of government (national, provincial and local).

The second variance that was analysed was society, which showed that the government must attend to the specific phenomena of unemployment, inequality and poverty. The government elite's involvement in protest action must also be considered. Additionally, police are understaffed, losing qualified and experienced members monthly; thus, they cannot control protests in the country efficiently. These past protests, while used to show the public's frustration with the ANC's poor governance, severely impacted the country's stability, many people lost their lives, and billions of rands of infrastructure were damaged and destroyed.

The third variance in the framework was security. This study assessed national security versus people's security separately, to obtain a better observation of the phenomena. The findings of the analysis showed that the responsibilities of an intelligence agency must focus on every aspect of the security cluster (national security) from a human security perspective. The crime levels in SA were one of the aspects that prominently stood out as a critical threat and risk for the government due to the involvement of foreign role-players. In addition, organised crime is something the whole government must focus on urgently. Thus, crime impacts both the government and its citizens through governance, security, and the economy of the country. Furthermore, crime often operates over country borders and involves neighbouring countries, and cooperation must be coordinated over long distances, prolonging these types of investigations, legal procures and arrests. In addition

to crime, SA has numerous problems relating to security. These include energy, water and food security, as well as issues with violent protests, crime (including organised crime) and xenophobia. However, xenophobic attacks threaten immigrant communities which tends to lead to international relations being blemished between SA and the countries whose citizens are involved. These security aspects usually influence the image of SA internationally, which impacts economic growth.

The analyses in the chapter showed that the four variances in the framework could not be studied separately because they all inter-relate with each other - poor governance impacts society, security, and the economy. The last (fourth) variance, economy, could be the glue holding all of these variances together. In addition, political risk is not easily analysed and explained but a general overview of SA's instability was provided. Based on this overview, the researcher feels that it does not matter which scenario you choose, these variances will always cause some instability.

Lastly, the study has found that IRM processes lend themselves to using different tools and methods to reach an adequately formulated conclusion. In this process, different indexes, barometers, analysis data, management tools and methodologies were used to draft four plausible scenarios that could inform the policy-maker or clients. From the analyses, the second scenario (Muddle Through, half-empty pot) is the most likely for SA. In the scenario, the ANC wins the 2024 election and everything remains relatively the same in terms of poor governance, unemployment and cadre deployment. SA will be threatened by electricity and water shortages, which will hamper any positive growth and investments in SA.

Furthermore, this chapter informed the use of these multi-tools and data, which shows that an IRM can be successfully applied in the intelligence environment of any political regime. However, this study believes that the SA government will not be interested in implementing this type of IRMF because it puts more control measures in place, and there will be better oversight of the IC.

CHAPTER 6: EVALUATION, RECOMMENDATIONS AND CONCLUSION

... the classified and unclassified versions of the Annual Threat Assessment submitted ... devote far more attention to problems and perils than to opportunities to shape events. This emphasis is understandable, but it is also unfortunate because it obscures one of the most important functions of the IC and causes both analysts and agencies to devote too little attention to potential opportunities to move developments in a more favourable direction. (Fingar, 2011:1)

6.1 Introduction

This final chapter will conceptualise and summarise the findings of the research. It will examine whether the research objectives were reached and if the research questions were sufficiently answered. The constant reports of intelligence failures have placed intelligence agencies under severe pressure to make the necessary changes to their functions, processes, and structures. This study has demonstrated that it is not necessary for agencies to make a revolutionary change to their practices but to keep up with the new developments in technologies, analytical and collection methods, to gain the necessary knowledge regarding IRM. These aspects will assist these agencies in identifying the necessary, trusted sources of data and information, better-formulated intelligence products, the same scientific knowledge and consensus on the processes to be followed, knowledgeable policy-makers, and a due decision process. It will further direct the intelligence framework in SA to implement already properly designed communication channels and processes, in order to take up their vital role in a democratic state by informing the policy-maker/client through better-constructed intelligence products that enhance the national security environment.

Within this chapter, the constructed IRMF will inform the intelligence regime that not all their intelligence processes need to be changed radically, as mentioned above (International Journal of Intelligence and Counter-Intelligence, 2007:3-4). Lahneman states that: *Some aspects of the intelligence enterprise will indeed need to transform, but other parts can continue to evolve, and others will remain essentially unchanged*. Furthermore, this chapter will make additional recommendations toward applying an IRMF within an intelligence context and address future research and recommendations for using an IRMF to enhance intelligence reporting in SA.

6.2 Study Overview

The study planned to explore and evaluate IRMFs and intelligence risk threat assessment modules to advise on which of these frameworks and modules will benefit the intelligence regime to enhance

national security and good governance. The dissertation focuses on an IRMF, which has not been studied clearly as a field of study before. Some studies indicate that RM should be used to enhance intelligence processes, specifically the intelligence analysis function. Therefore, the research study explores, describes, and explains the intelligence and RM phenomena through comparative and descriptive research methods. During the literature and data study, primarily open-source/overt information (books, journals, internet, and articles) was used to ensure that the dissertation is available and not classified due to the secret nature of the intelligence environment. Therefore, the dissertation unfolds its methodological approaches as described in the paragraphs below.

Chapter One explored the literature and data available on the three prominent phenomena in the study (intelligence, RM, and national security) and formulate a proposal on how this dissertation would investigate the research study. The most important part of Chapter One was the literature study due to the new field of study (IRM) that applies to this *study*. There are limited studies devoted to exploring the diversification of the meanings, and there is a lack of (meta-) risk theory that explains the co-existence of intelligence, RM and national security. Small details and explanations regarding the field were identified in different sources of information (books, journals, articles, and internet websites) which ensured that the *study* had an extensive bibliography. The dissertation is not classified, indicating that sensitive and classified materials were not considered for investigation and analysis.

Chapter Two defined and explained the definitions, concepts, functions, and purposes of intelligence, RM, and national security through conceptualisation and theoretical analysis from a meta-theoretical perspective to better understand the IRM field of study. The most critical understanding of the three phenomena' inter-relationship/interaction/work is explained, and what theories influence the framework developed in Chapter Three. Furthermore, the chapter discussed the changes necessary to ensure a process that will enhance the end product, to provide the necessary intelligence to the policy-makers to make informed decisions regarding threats, risks, vulnerabilities, and opportunities.

Chapter Three explored all relevant intelligence and RM frameworks to conceptualise and develop an IRMF for the SA environment. To ensure that these frameworks complied with the country's legal framework, they were conceptualised from a democratic perspective. Therefore, when investigating these phenomena, Walsh's description of an intelligence framework was used to form the primary analysis. The methodological approach of these frameworks ensured that the theories of frameworks and concepts were better understood and an IRMF could be conceptualised.

Chapter Four used exploratory and historical research methods to explain, describe and evaluate the development and implementation of intelligence, RM and national security in SA. This research ensured that most of the problems and shortcomings in the SA intelligence environment were

identified, and recommendations to enhance these aspects were explained and assessed. These aspects provided the necessary information to design and create the necessary IRMF and knowledge to evaluate SA intelligence frameworks' compliance with the conceptualised IRMF.

Chapter Five indicated the IRMF processes to create an assessment of SA's instability aspects. Scenario planning and tool building was used to analyse the SA environment and formulate plausible scenarios. These scenarios were further analysed to determine which was most probable for SA. These analyses showed that an IRMF can be implemented in SA's IC and which of the tools for assessment can be successfully used in these processes.

The final chapter examines whether the research objectives have been reached and if the research questions were sufficiently answered. It will also make proposals for further studies on the research topic of IRM studies as a field of study. To evaluate if the study complied with these objectives and questions, it will describe the successes and enhancements of the study.

6.3 Evaluation of the Research Objectives and Secondary Questions of the Study

The study has approached a new field of study (IRM) from a meta-theorical research approach which will be analyse and evaluated in this section.

6.3.1 Introductory to an evaluation of the study

A mainly explorative and qualitative research methodology was used in this study. Maree (2011:51) describes qualitative research as a *research methodology concerned with understanding the processes and the social and cultural context which underlies various behavioural patterns and is mostly concerned with exploring the 'why' questions of research*. Through deductive reasoning, the study established an IRMF and techniques/methods enhancing the intelligence risk analysis process to provide timely forewarning and strategic threat intelligence to the policy-maker/client. Although this study, as referred to in the title, mainly focused on an explorative perspective approach, it also implemented explanatory and descriptive research approaches. This study applied a meta-theoretical and theoretical approach to understanding the different interdisciplinary concepts and theories applicable to this research topic. Furthermore, the study evaluated the secondary objectives and questions below:

- Through explorative investigation and analysis, define and describe the theories influencing the study to address the inter-relationship between intelligence, uncertainty, risk, and national security in an IRM field of study;

- Conceptualise and construct an IRMF;
- Describe and explain the historical development and application of IRM in the SA context; and
- Assess and evaluate the application of an IRMF for SA and its enhancement of national security.

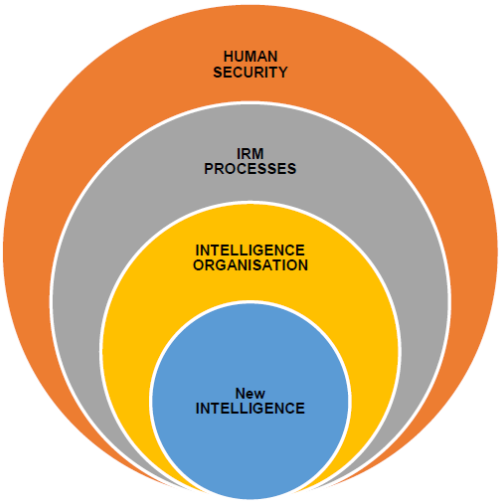
6.3.2 An Intelligence Risk Management field of study

The first objective of this study was to determine the inter-relationship between three phenomena - intelligence, RM and national security. This inter-relationship was conceptualised by determining the core aspects of setting a standardised vocabulary and standards for the field of study. Understanding IRM vocabulary and standards, it became clear that there is a need to change the traditional intelligence field of study to accommodate RM. The *study* has approached the study from a meta-theoretical perspective to study these phenomena and their inter-relationship. This approach provided the necessary changes in the new field of study. The study followed the meta-theory, as Ritzer (2001:17-18) and Bay (2007:19) described: *the theories behind the definitions, purposes, concepts, and processes of the phenomenon to clarify the distinction*. These aspects directed the study, and all three of these phenomena were approached to understand and obtain the necessary knowledge of each and how they will inter-relate with each other in an IRM field of study.

This study needed to use Ritzer's (2001:18) arguments regarding the meta-theory outcomes because it had to determine whether an IRM field of study will deliver a better and enhanced framework for the intelligence environment. The study, through comprehensive conceptualisation, comparison of some different approaches and structuring of these three phenomena (intelligence, RM and national security) concepts, found that several different approaches and applications deliver new theories, end products and a change in the theoretical perspective in IRM.

The above considered, more clarity is given by Gill and Phythian (2018:47), when they quoted Der Derian's (1992:27) views regarding *what is needed in intelligence studies is a meta-theory that would consider the fact that 'ambiguous discourse, not objective truth, is the fluctuating currency of intelligence. The indeterminacy of what is seen or heard, aggravated by encoding, decoding, and, possibly, deception, plus the gulf between what is said and what is meant, requires an approach rooted more in rhetoric than reason. This approach – inter-textualism – 'aptly covers the field of intelligence, where there is no final arbiter of truth, meaning is derived from an inter-relationship of texts and power is implicated by the contingent nature and ambiguity of language and other signifying practices.* Gill and Phythian further quote Der Derian (1992:46): *the texts to be analysed are not just the factive ones of national security studies, but also the fictive literature of international intrigue that 'produce meaning and particular legitimate forms of power in their relation to each other*. This study determined these aspects in Chapters Two and Three.

In conclusion, IRM needs to be approached from a meta-theory approach as described above by Ritzer (2001), Bay (2007), Gill (2018), Phythian (2018), and Der Derian (1992). IRM can broadly be described, based on a presumption about the world. These presumptions are based on understanding the phenomena intelligence, RM and national security. These will all be applied in the changing intelligence environment as described in Chapter Two. These presumptions are fundamental to understanding why intelligence, RM, and national security are defined and why some definitions prevail. It notably shows that these phenomena can inter-relate and describe why we have them, why we need them, their purpose, and how we should use them in one sub-study field of IRM. These concepts are of great importance to the field of intelligence in this changing world. Furthermore, these findings show that change is needed in the intelligence environment and that this change needs to align with our changing world. This study also provided the necessary analysis that combines the three phenomena and further the theories, which place the phenomena in the basic definition of intelligence which can be viewed in the graphic below.



Source: Researcher's construct

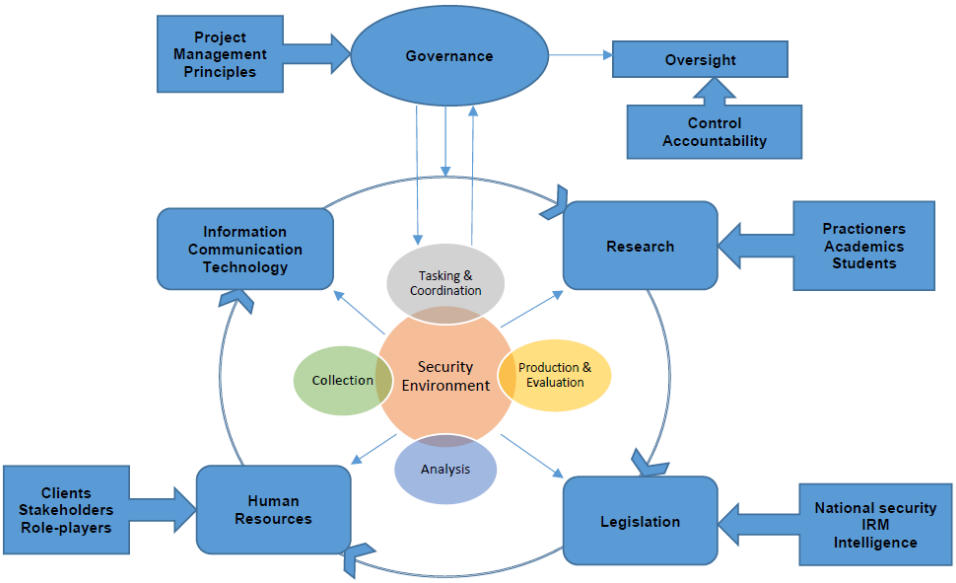
Figure 29: New Intelligence Approach

These analyses prove that with changes made, IRM can provide the necessary national security products to inform clients/policy-makers. Furthermore, the study showed that national security needs to be handled from a human security perspective, which will provide the necessary IRM products, including all the threats, risks, vulnerabilities, and opportunities.

6.3.3 Explore an Intelligence Risk Management Framework

The study conceptualised an IRMF by investigating Walsh's (2011) framework and how it could influence the field of IRM. That brought a better understanding of the intelligence processes to provide

an enhanced product. These national security products will inform the policy/decision-makers to manage uncertainty and risk in their environment. The frameworks mentioned above have clarified the core areas in the intelligence processes that need to change, as reflected in the figure below These frameworks' impact on the changing intelligence processes is reflected in Walsh's (2011) adapted figure below.

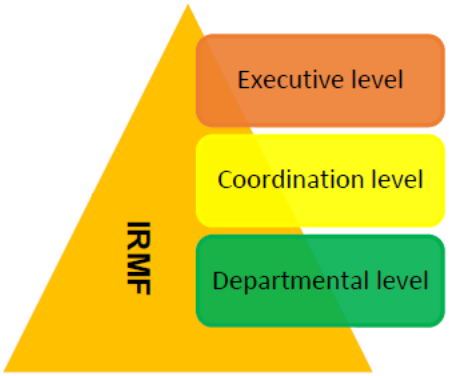


Source: Adapted from Walsh (2011:148)

Repeated Figure 10: Components of an effective intelligence framework

This graphic clearly shows how the new intelligence processes will influence the traditional processes which are followed internationally. This study's impact on the conceptualised IRMF and the changes that need to be implemented will influence the traditional framework. Every aspect of that framework will need some change to comply with the IRMF as conceptualised by this study. The graphic also reflects some core aspects needed to create and implement an IRMF. These aspects are i) project management principles; ii) good governance with oversight; iii) good coordination; iv) change intelligence processes; v) well-trained and skilled practitioners; and vi) ensuring a legislative framework that captures the intelligence, IR and national security concepts in the implementation of an IRMF.

The study showed that an IRMF should function on three specific levels, as reflected in the figure below. Each one of these levels was defined; some levels have been allocated specific tasks, responsibilities, and accountabilities to the structure in these levels.



Source: Researcher's construct

Figure 30: IRMF Levels

The above-defined levels for the IRMF were compared with democratic principles as researched by DCAF (2006 – 2022). This investigation revealed that the executive level must be structured as follows:

- Presidential, head of state or prime minister responsibilities and accountabilities;
- Ministerial responsibilities;
- Parliamentary and oversight institutions/committee's responsibilities; and
- Committees, councils and commissions (NSC/committee, parliamentary committees).

The coordinating level found that most democratic countries do not have a specific governmental structure according to legislation to coordinate intelligence or IRM. Most countries do have coordination built into their intelligence environments. These coordination structures coordinate all intelligence products and information that must be sent to the executive levels. Dedicated communication lines were found and built into the conceptualised IRMF. The IRMF sees coordination as a national coordination structure to which all intelligence products or production will flow for coordination to the executive level.

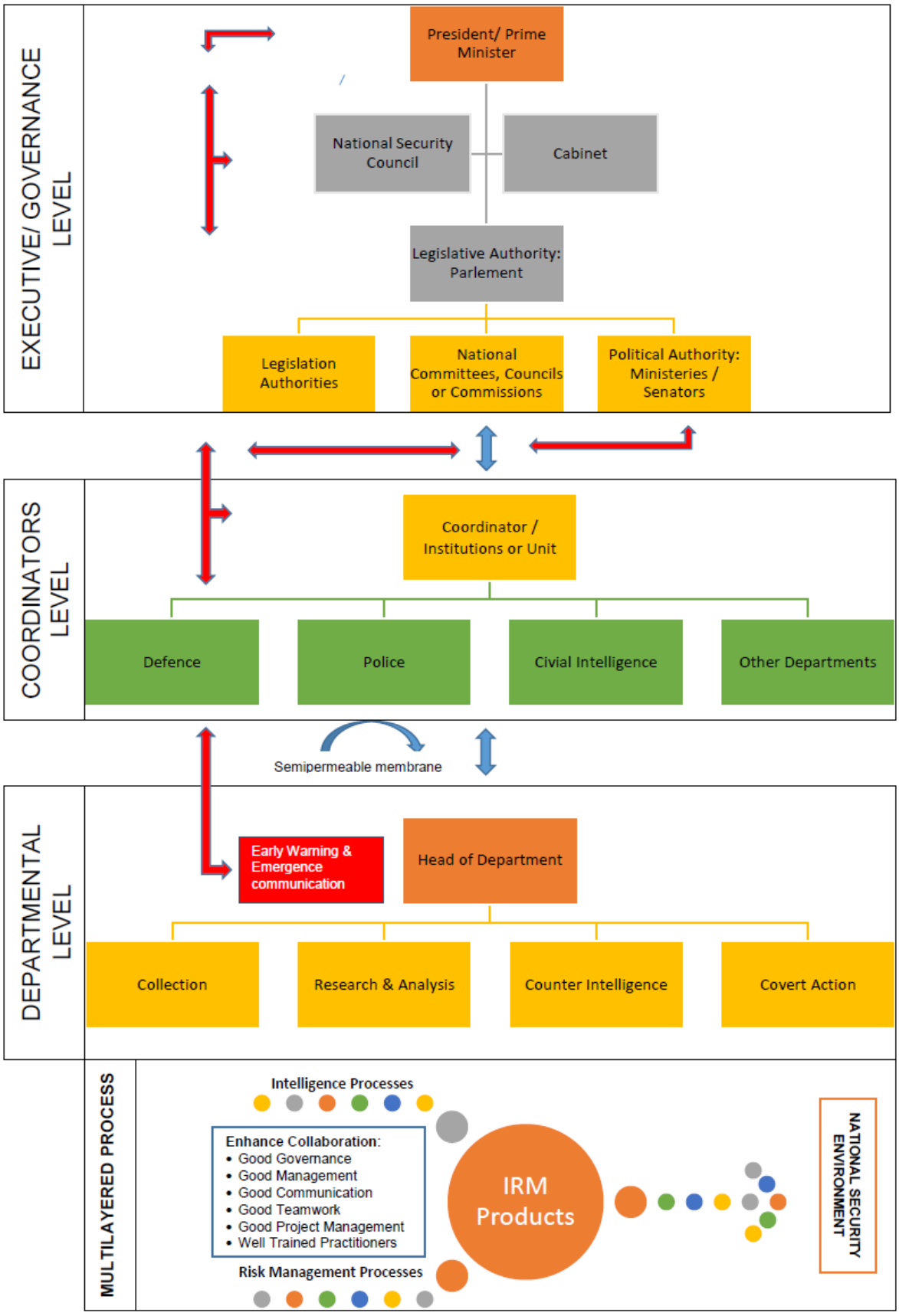
At the departmental level, the study found that the intelligence processes had to be changed to ensure that a multi-layered intelligence process could be implemented. Figure 14 (Section 3.7.3) reflects the findings and proposed structure on this level for implementation. Therefore, this study postulates its argument that intelligence agencies need to change their intelligence processes to a multi-layered process that will ensure integration and a holistic approach. The process is also described by Lowenthal (2009:67) as *any one intelligence process issues likely arise (the need for more collection, uncertainties in processing, results of analysis, changing requirements) that cause a second or even third IRM process to take place. Ultimately, one could repeat the process lines repeatedly to portray continuing changes in any of the various parts of the process and the fact that policy issues are rarely resolved in a single neat cycle. It gives a much better sense of how the intelligence process operates*

in reality. Additionally, the study found that an IRMF will enhance several aspects of the intelligence environment and IRM products, including:

- Good governance;
- Good management;
- Good communication and lines of communication;
- Set communication standards and vocabulary;
- Good coordination;
- New intelligence processes, which include IRM;
- Good teamwork and project management; and
- Well-trained practitioners.

To summarise the above advantages and to give an overview of the conceptualised IRMF, the figure below projects the framework. The study conceptualised an IRMF that can be used to evaluate the current reality of SA's intelligence framework and reflect all the necessary theoretical and conceptualised aspects of a properly designed framework. However, the conceptualised IRMF needs improvement that could only be obtained through a more in-depth meta-theoretical study of other relevant theories and further developed doctrine for IRM. The latter is currently non-existent within the SA context.

The practitioner is required to improve current practises and extend existing theory and knowledge to enable adjustment to an ever-changing political, economic and social world. For such an IRMF to be functional, it also requires constant refocus and the ability to adapt to the only known concept of change, which remains the only constant.



Researcher's construct

Repeated Figure 15: Conceptualised IRMF

6.3.4 Describe and explain the historical development and application of intelligence risk management in the South African context

The methodological approach in this part of the study was directed by analysing the SA intelligence framework through comparative analysis against the conceptualised IRMF of Chapter Three. Firstly, a historical study was done to determine the status of intelligence, RM and national security in SA. A summary captured in Figure 16 (Section 4.2) reflects the historical information and development of these three phenomena in the SA context. It was found that SA was not very far behind the rest of the developed world regarding their development, as they were developed and reflected well in structure, legislation, and research.

Due to intelligence functioning under secrecy and documentation not regularly being unclassified, this research only used open-source information, including books, journals, available structural information, website information regarding intelligence and news paper reports regarding intelligence and national security, to avoid classification of the dissertation. The information available provided the necessary context to explore and assess SA's intelligence regime. In Chapter Four, Figures 17, 19 and 20 clearly showed that SA could implement an IRMF. This analysis showed that SA complies with all different levels of Chapter Three's conceptualised IRMF (structures and legislation). In addition. the original drafters of the Constitution, intelligence legislation, the White Paper and structures have included all the principles, standards and coordination aspects reflected in Chapter Three's conceptualised IRMF. However, several problems have been identified that must be corrected to ensure that SA fully complies with the aspects of an IRMF. These aspects were captured in Chapter Four and can be summarised as follows:

- The functionality of the NSC. It has not functioned for some time and was only re-activated by President Ramaphosa in 2020; (SA Government Gazette 2021)
- Some Ministers of Intelligence had become involved in the civilian intelligence agency's operations. They did not (or want to) understand the roles of ministers and government departments; (HLRP, 2018:66-68)
- The distinct separation of powers that needs to be ensured by departmental levels in policy formulation and decision-making is critical. Lowenthal (2009:5) argues that intelligence agencies must not become involved with the executive governance and policy formulation functions because it creates a problem of agencies being politicised or influenced by the policy-makers. Reports from the HLRP indicated that the civilian intelligence agency (SSA) is politicised and the ruling party factions are embedded in the agency;
- Poor management on all levels will hamper the implementation of an IRMF. Parliament's Cabinet and oversight committees are not doing their work accordingly, and no actions are taken against departments not reporting to these committees;

- The coordination of intelligence is not functioning correctly in SA. It is also reflected in the feedback report on July 2021's violent protests. The HLRP recommended that NICOC be placed under the Presidency, and its responsibilities must be reconfirmed with all the intelligence role-players;
- The human factor will hamper the implementation of the IRMF in SA because members are not adequately skilled, the placement of members is not well administrated, cadre deployment by the ruling party is rampant, and members do not understand the different roles and responsibilities of people and structures in government; and
- Historically, SA's IC did not implement or adhere to recommendations made by commissions, task teams, and panels, leaving doubt about implementing the IRMF. The study showed that an IRMF would ensure the implementation of more than only the framework. It would enhance the intelligence environment's good governance, management, communication, and training.

The study provided the necessary comparative analysis and achieved the objective of conceptualising an IRMF for implementation in SA. The current structure available on the ministerial website of the SSA was adapted by the study in Figure 20 (Section 4.6) - the study's findings are reflected in this structure with a legislation framework included.

6.4 Assess and Evaluate the Application of an Intelligence Risk Management Framework for South Africa and its Enhancement of National Security Through Plausible Scenarios and Recommendations

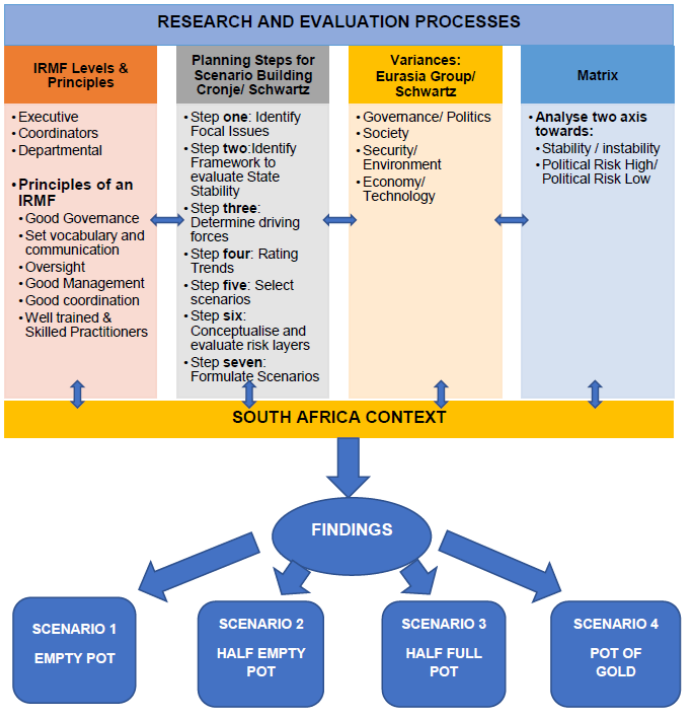
In Chapter Five, the use of an IRM process in the SA political environment was applied to determine if the process could be successfully implemented to deliver plausible scenarios regarding the stability or instability of SA. From a political perspective, the first aspect or question to be answered was 'what you understand of these two phenomena' (stability and instability). The study analysed the two concepts and found no clarity on how they must be defined and approached. The dissertation thus concludes that a broad definition will benefit the IRM approach. Therefore, in this study, stable states are characterised by government capacity, legitimacy, a legal/rational state, democracy and human rights, and development and economic integration.

The study combined Cronje (2014) and Schwartz's (1996) principles and steps to determine how to compile the scenario steps and format. The study applied scenario analysis planning and building science to analyse the information available in Chapter Five. The following steps were applied:

- Step One: Identify focal issues regarding stability and instability in SA;
  - Political risk is the core aspect of stability index analysis;
  - The SA environment from an IRM perspective;

- Step Two: Eurasia Political Risk Index – Framework to evaluate state stability;
- Step Three: Determine the driving forces which can change these aspects in the SA environment through these four variables;
- Step Four: Rating trends in the SA context from an IRMF perspective;
- Step Five: The selection of scenarios;
- Step Six: Conceptualise a framework for risk layers on SA's political in/stability index;
  - Government;
  - Society;
  - Security;
  - Economy/technology; and
- Step Seven: Construct plausible scenarios for the SA context.

The above planning and building blocks of scenario science were followed, and four very specific scenarios were formulated, of which the second was identified as the most probable scenario to materialise in SA. In short, the ANC wins the 2024 election and everything remains relatively the same in terms of poor governance, unemployment and cadre deployment. SA will be threatened by electricity and water shortages, which will hamper any positive growth and investments in SA. A summary of the operationalisation of the conceptualised IRMF used in the study in the SA context is shown below.



Source: Researcher's construct

Figure 31:Summary of the operationalisation of the conceptualised IRMF used in the study

6.5 Concluded Findings and Contribution of the Study

This research's focus was on a new IRM field of study. The field of study is not identified as such in intelligence studies, which is a sub-field of study under political science. IRM as a study field brings three phenomena together into one field of study under intelligence study and determines the inter-relationship of these phenomena through a meta-theoretical approach to understand and obtain the necessary knowledge of these three sciences. IRM must be approached from a meta-theory approach as described by Bay (2007), De Derian (1992), Gill (2018), Phythian (2018), and Ritzer (2001). IRM will be broadly described based on a presumption about the world. These presumptions will be based on understanding the phenomena of intelligence, RM, and national security, which will be applied in the changing intelligence environment described in Chapter Two (Section 2.6). These presumptions are fundamental to understanding why intelligence, RM, and national security are defined and why some definitions in these three fields prevail. Notably, these phenomena can inter-relate and the field can describe why we have them, why we need them, their purpose, and how we should use them in IRM.

Arad (2008:43-49) describes the inter-relation between intelligence and RM from a surprise attack perspective. The author argues that some of the recorded intelligence failures in history clearly show that something 'went wrong' and could have been prevented if RM principles were applied. This dissertation determined that a moderate change approach must be followed. These changes in intelligence will be needed to ensure the inter-relationship between intelligence and RM. Furthermore, Arad (2008) argues that intelligence uses some of the 'risk assessment and management fundamentals' in the tactical, operational environment. He also indicate that intelligence practices already specifically use *probabilistic measurements, evaluation of risk and the use of scenarios, there is a wide use of explicit risk-control and management tools, such as backup systems, and risk reduction via diversification and redundancy*. This motivates the use of RM inter-related with intelligence, which should not create a problem in the intelligence processes because their practitioners and management are trained in 'probability thinking' in early warning applications.

This research and analysis regarding these three phenomena included an advantageous literature study regarding this field, which showed that vocabulary and standards are needed to enhance the practical implementation of an IRMF. The study postulated a vocabulary to ensure a better understanding of the theories, concepts, and principles. The study furthermore identified several aspects that bind intelligence and RM in an IRM process, which can be summarised as follows:

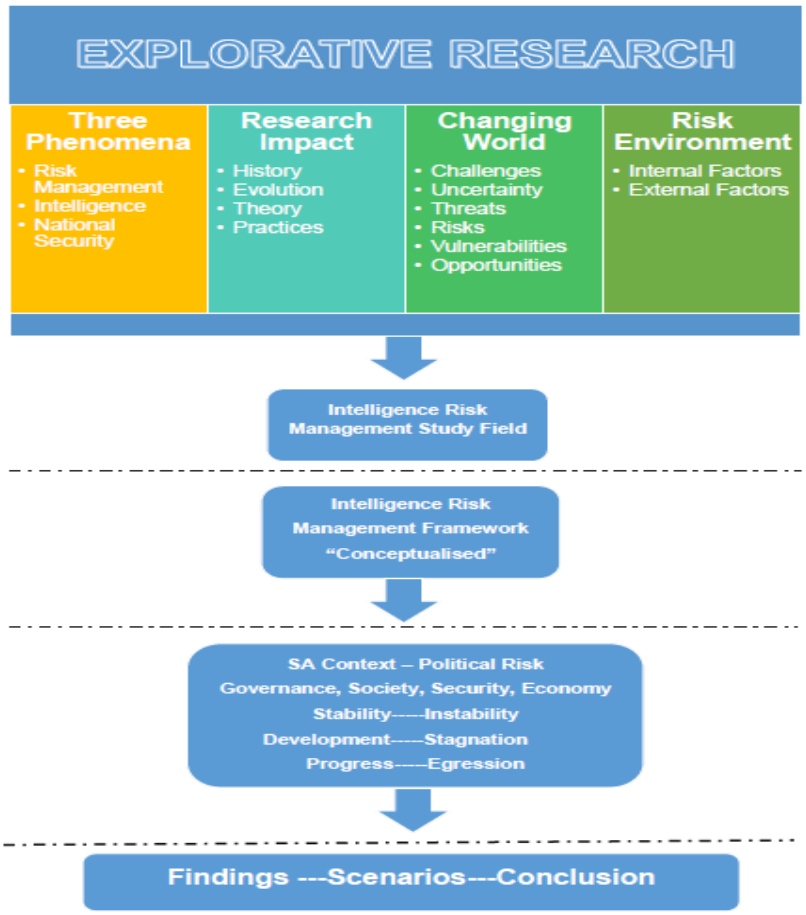
- ORM is recommended in the application of RM in the sequential process;
- New ways of data/information collection and management should be applied in the modern world;
- Different individuals assess likelihood (probability) in different ways;

- Existing methods of applying intelligence and RM need to change;
- The primary objective of these phenomena will encourage managers to be sensitive to other forms of data; and
- Intelligence inputs into the decision-making process used to reduce ***uncertainty***, ***identify risks*** and ***opportunities.***

This study has also identified that practitioners will have practical problems when they want to implement an IRM process, summarised as follows:

- There is no written or promulgated doctrine on IRM;
- Arad (2008:43-49) argues that there are specific aspects/'obstacles' regarding the types of risks (internal and environmental) that need different tools to assess these risks, creating a problem in the intelligence processes;
- The intelligence processes viewed environmental risks as threats from the external environment and failed internal processes as operational risks from people, processes, and technology;
- These aspects of environmental risks 'lower the relevance of statistics and probabilistic distributions' in the RM processes; and
- Two different structures with different tools analyse the abovementioned risks (environmental and internal operational risks).

The study already provided an excellent basis to formulate the necessary doctrine to implement and apply an IRM process in intelligence agencies through the research mentioned earlier. Furthermore, the study has identified the changes needed in intelligence, RM and national security to successfully perform further research that will enhance the field of study and find all the aspects of an IRMF that need clarity in a specific agency. The figure below shows the overall summary of this study.



Source: Researcher's construct

Figure 32: Overall summary of an explorative perspective of an IRMF for SA

6.6 Final Recommendations for Future Studies and Development

Through this study, several future study areas were identified, enhancing the intelligence study field, and providing better knowledge and understanding of theories and concepts. The changes in intelligence, RM, and national security after the Cold War era tempted several states, institutions, and specific intelligence agencies to convert to risk intelligence practices to ensure they could manage uncertainties, risks, vulnerabilities, and opportunities. All three phenomena (intelligence, RM, and national security) cannot be clearly defined and there is no theoretical approach to these phenomena or theories which would direct researchers to gain more knowledge or a better understanding of their inter-relationship in the field of intelligence studies. Bay (2007), Gill (2012), Gill and Phythain (2018), Phythian (2012), and Warner (2009) indicate that a more meta-theoretical approach in intelligence studies must be followed to gain clarity and breach the shortcomings in intelligence studies.

Furthermore, Zinn (2009:8) argues that *there are diverse views and interpretations of risk. In the literature, the risk is often regarded as 'analysis', 'social constructs', 'feelings' and so forth*. Due to limited studies devoted to exploring the diversification of the meanings of this phenomenon, this study

proposes that more studies be devoted to research (meta-) risk theory that explains their co-existence. Thus, the meta-risk theory will enhance the understanding of the essential aspects of the field of intelligence.

Equally important from the above notion is that intelligence inputs into the decision-making process aim to reduce ***uncertainty***, ***identify risks*** and ***opportunities***, and, by doing so, deepen understanding so that those with policymaking responsibilities will make more informed decisions. These aspects regarding RM should be further investigated as to how they inter-relate with intelligence processes. This combined with meta-theory studies will enhance the IRM sub-study field. These aspects are becoming increasingly crucial for intelligence service delivery.

According to Arad (2008:43-49), *intelligence practices already specifically use probabilistic measurements, evaluation of risk and the use of scenarios, there is a wide use of explicit risk-control and management tools, such as backup systems, and risk reduction via diversification and redundancy*. This motivates the use of RM inter-related with intelligence. The researcher firmly believes in Arad's proposal, namely that the IRM study field needs to provide doctrines and policies on how to implement an IRMF in a country. These doctrines and policies must be investigated, and standardised products must be developed. Since no doctrine or policies are available on the phenomenon, the proposed theoretical framework of this study may be a valuable tool for academics to understand these antecedents in the future and improve on them.

BIBLIOGRAPHY

Africanews. Mumbere, D. 04 October 2019. Xenophobic attacks in South Africa embarrassed continent: Nigeria's Buhari. https://www.africanews.com/2019/10/04/buhari-visits-south-africa-on-a-mission-to-secure-nigerians-welfare// Date of access: 28 Sep. 2022

Africa S.E. and Mlombile S. 2001. The Transformation of The South African Intelligence Services. Paper presented to the Roundtable on the Reform of the Guatemalan Intelligence Services. Boston, MA: Harvard University Law School.

Africa, S.E. 2009. South African intelligence services: a historic perspective. (*In* Africa, S.E. & Kwadjo, J., *eds*. Changing Intelligence Dynamics in Africa. Birmingham: GFN.SSR. p. 78–79).

Africa, S.E. 2011. The Transformation of the South African Security Sector: Lessons and Challenges. *The Geneva Centre for the Democratic Control of Armed Forces*, Geneva. www.dcaf.ch/publications Date of access: 10 Oct. 2018

Afrobarometer (2022). South Africa Website https://www.afrobarometer.org/countries/south-africa/ in partnership with Institute for Justice and Reconciliation (IJR) in South Africa. Date of access: 30 Sep. 2022.

Agrell, W. 2002. When everything is Intelligence - Nothing is Intelligence. CIA: The Sherman Kent Centre for Intelligence Analysis, 1(4):1-6. https://www.cia.gov/library/kent-center-occasional-*papers*/vol1no4.htm. Date of access: 15 Nov. 2018.

Ake, C. 1973. Explaining Political Instability in New States. *The Journal of Modern African Studies*, 11(3):347-359. http://journals.cambridge.org/MOA Date of access: 30 Jul. 2022.

Allison, G. T. 1971. Essence of decision; explaining the Cuban missile crisis. Boston. MA., Little Brown.

Arad, U. 2008. Intelligence Management as Risk Management: The Case of Surprise Attack. (*In* Bracken, P. et al. 2008. Managing Strategic Surprise (Lessons from Risk Management and Risk Assessment). London, Cambridge University Press. p.43-77

BIBLIOGRAPHY

Bar-Joseph, U. and Kruglanski, A.W. 2003. Intelligence Failure and Need for Cognitive Closure: On the Psychology of the Yom Kippur Surprise. *Political Phycology Journal*, 24(1) p.75 – 99.

Basel Committee on Banking Supervision (BCBS), 1990: RMA, British Bankers' Association, ISDA, PricewaterhouseCoopers, *Operational Risk –the next frontier*, 1999. http://www.logicmanager.com/pdf/operational_risk_management.pdf Date of access: 02 Sep. 2019.

Bay, S. 2007. Intelligence Theory: A Literary Overview. Lund University, *Research Policy Institute*, FPO 026. Spring Term 2007. https://www.researchgate.net/publication/342765151_Intelligence_theories_-_a_literary_overview Date of access: 22 Sep. 2017.

Beale, R. 2008. Report: The Independent Review of Australia's Quarantine and Biosecurity Arrangements Report to the Australian Government. http://www.ag.gov.au/cca Date of access: 16 Oct. 2019)

Bearne, S., Oliker, O., O'Brien, K.A., Rathmell, A. 2005: National Security Decision-Making Structures and Security Sector Reform. Prepared for the United Kingdom's Security Sector Development Advisory Team. Santa Monica, RAND Corporation.

Betts, RK. 1978. Analysis, War, and Decision: Why Intelligence Failures are inevitable. World Politics, Vol. 31, No. 1 (Oct. 1978), p. 61-89, Cambridge University Press.

Betts, RK. 1982. Surprise Attack: Lessons for Defence Planning. Washington, D.C: Brookings Institution.

Betts, R.K. 2009. Analysis, war, and decision: why intelligence failures are inevitable. (*Ed. By* Gill, P., Marrin, S. and Phythian, M. 2009. In Intelligence Theory: Key questions and debates. Studies in Intelligence. London: Routledge

Bhattacherjee, A. 2012. Social Science Research: Principles, Methods, and Practices, 2nd edition, *Collection.* Book 3. http://scholarcommons.usf.edu/oa_textbooks/3 Date of access: 08 Nov. 2019.

Bracken, P. Bremmer, I. and Gordon, D. 2008. Managing Strategic Surprise (Lessons from Risk Management and Risk Assessment). London, Cambridge University Press.

BIBLIOGRAPHY

Blunden, T. and Thirlwell, J. 2010. Mastering Operational Risk. Harlow: Pearson Education.

Blunden, T. and Thirlwell, J. 2013. Mastering Operational Risk. 2nd edition. Harlow: Pearson Education.

Born, H. and Caparini, M. 2007. Democratic Control of Intelligence Services. Hampshire, Ashgate.

Born, H. and Leigh, I. 2007. *Geneva Centre for the Democratic Control of Armed Forces*, (DCAF), Policy Paper – №19, www.dcaf.ch/publications. Date of access: 30 Aug. 2017

Bracken, P, 2020. Intelligence and Risk Management. Zürich *Foreign Policy Research Institute*.

Bremmer, I. 2005. Managing Risk in an Unstable World. *Harvard Business Review, Economics*, Jun. 2005. https://hbr.org/2005/06/managing-risk-in-an-unstable-world Date of access: 20 Nov. 2019

British Bankers Association Gold database, 2022. https://www.bba.org.uk/news/statistics/operational-risk-statistics/global-operational-loss-database-gold/#.XWFtwxuP7IU Date of access: 29 Sep. 2022

BusinessDay, Ensor, L. Real progress is being made to avoid greylisting, 24 Oct. 2022: https://www.businesslive.co.za/bd/economy/2022-10-24-real-progress-is-being-made-to-avoid-greylisting-says-momoniat/ Date of access: 26 Oct. 2022.

Business Insider SA. Brown, J. 17 Feb. 2020. Xenophobia isn't keeping immigrants out of SA –here are the latest, if contentious, numbers. https://www.businessinsider.co.za/immigrant-numbers-for-south-africa-are-still-rising-despite-xenophobia-and-violence-2020-2 Date of access: 5 Nov. 2022.

Businesstech, 14 Sep. 2021. Intelligence report reveals ‘shocking reality’ around the interception of communication in South Africa. https://businesstech.co.za/news Date of access: 11 Aug. 2022.

Businesstech, 2 Nov. 2021. 3 scenarios for South Africa – and where we’re heading right now. https://businesstech.co.za/news/banking/533650/3-scenarios-for-south-africa-and-where-were-heading-right-now/ Date of access: 11 Aug. 2022.

BIBLIOGRAPHY

BusinessDay, Ensor, L. 24 Oct. 2022, Article online: Financial Task Force - Real progress is being made to avoid greylisting, says Momoniat. https://www.businesslive.co.za/bd/economy/2022-10-24-real-progress-is-being-made-to-avoid-greylisting-says-momoniat/ Date of access: 15 Oct. 2022.

Buzan, B. 1991. New Patterns of Global Security in the Twenty-first Century. *International Affairs* (Royal Institute of International Affairs 1944-), 67(3): 431-451. Oxford University Press. Date of access: 30 Oct. 2018.

Buzan, B., Wæver, O. and de Wilde, J. 1998. Security: A New Framework for Analysis. Colorado, Lynne Rienner.

Cavelty, M.D. and Mauer, V. 2009. Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence. Security Dialogue 40(2). http://sdi.sagepub.com/content/40/2/123 pp. 123-144. Date of access: 25 Aug. 2017.

Cawthra, G. 2013. National Security and the right to information: the case of South Africa. www.right2info.org/resources/national-security-and-the-rti-in-south-africa. Date of access: 18 Oct. 2018.

Chipkin, I., Vidojević, J., Laurence Rau, L. and Saksenberg, D. (2022). The Near Future of South Africa: Protest and Political Stability, The Government and Public Policy (Gapp). https://issafrica.org/research/southern-africa-report/dangerous-elites-protest-conflict-and-the-future-of-south-africa Date of access: 20 Oct. 2022.

Chtouki, Z. and Raouf, R. 2021. The impact of political stability on economic performance in Africa: Evidence from 40 African countries. International Journal of Economics and Management Research, V.1, N°4, June-July 2021. (PDF) The impact of political stability on economic performance in Africa: Evidence from 40 African countries (researchgate.net) Date of access: 17 Nov. 2021.

Clark RM. 2003. Intelligence Analysis: A Target-Centric Approach. Washington DC: CQ Press.

Clark, RM. 2010. Intelligence Analysis A target-centric approach. 4th ed. Washington DC: CQ Press.

Classen, J.S. 2005. The craft of intelligence analysis and assessment: a training manual for intelligence analyst. Unpublished script. (SANAI)

BIBLIOGRAPHY

Clauser, J. 2008. An introduction to intelligence research and analysis. Maryland, MD.: Scarecrow Press.

Cleary, S. & Malleret, T. 2006. Resilience to Risk. Cape Town: Human & Rousseau.

Compact Oxford English Dictionary for Students, 2006. edited by Soanes, C. and Hawker, S., (eds.) Oxford: Oxford University Press.

COMEST, 2005. The Precautionary Principle (Paris: World Commission on the Ethics of Scientific Knowledge and Technology).
http://unesdoc.unesco.org/images/0013/001395/139578e.pdf4 Date of access: 03 Jan. 2020.

Concise Oxford Dictionary (1999). 10th edition. Oxford: Oxford University Press**.**

Constitution ***see*** South Africa

Covello, V.T. and Mumpower, J.L. 1985. Risk Analysis and Risk Management: An Historical Perspective. Society for Risk Analysis 5(2): 103-120. [PDF] Risk Analysis and Risk Management: An Historical Perspective (researchgate.net) Date of access: 03 Mar. 2019.

Cronje F, 2014. A Time Traveller's Guide to our next ten years. Cape Town: Tafelberg.

Cronje F, 2017. A Time Traveller's Guide South Africa in 2030. Cape Town: Tafelberg.

Cronje F, 2020. The rise or fall of South Africa. Cape Town: Tafelberg.

Dabari, IJ. & Saidin, SZ. 2014. A theoretical framework on the level of risk management implementation in the Nigerian banking sector: The moderating effect of top management support. *Procedia - Social and Behavioral Sciences* 164(2014):627 – 634. www.sciencedirect.com Date of access: 21 Sep. 2018.

Daily Maverick, Phiri, S. 07 Jul. 2022. Changing face of xenophobia in SA as government hesitant to take firm stand. https://www.dailymaverick.co.za/opinionista/2022-07-07-changing-face-of-xenophobia-in-sa-as-government-hesitant-to-take-firm-stand/ Date of access: 3 Nov. 2022.

BIBLIOGRAPHY

Daily Maverick, Dolley, C. 12 Oct. 2022. Irregular expenditure in police soars by 350%, Parliament hears. https://www.dailymaverick.co.za/article/2022-10-12-irregular-expenditure-in-police-soars-by-350-parliament-hears/ Date of access: 13 Oct. 2022.

Damodara, A. 2007. Strategic Risk Taking: A Framework for Risk Management. Upper Saddle River, NJ: Prentice Hall.

Daniels P. 2019. National Security Strategy Development - South Africa Case Study, Working Paper - Africa Centre for Strategic Studies. Publish online: https://africacenter.org/wp-content/uploads/2019/04/2019-04-NSSD-Case-Study-South-Africa-Defense-Policy-Review Date of access: 18 Jul. 2022.

Davies, PH. 2009. Theory and intelligence reconsidered. (In Gill, P., Marrin, S. and Phythian, M. eds. 2009: Intelligence Theory: Key questions and debates). Studies in intelligence. London: Routledge, p. 189-207.

DCAF. 2006 (03). Backgrounders Series: Contemporary Challenges for the Intelligence Community. backgrounders@dcaf.ch Date of access: 20 Dec. 2019.

DCAF. 2010. Backgrounders Series: National Security Councils. backgrounders@dcaf.ch Date of access: 20 Jan. 2020.

DCAF. 2015. Justice, Backgrounders Series: The Justice Sector, Roles and responsibilities in good security sector governance. backgrounders@dcaf.ch Date of access: 20 Jan. 2020.

DCAF. 2015 (SS). Backgrounders Series: The Security Sector. backgrounders@dcaf.ch Date of access: 20 Jan. 2020.

DCAF. 2015 (P). Backgrounders Series: Parliaments. backgrounders@dcaf.ch Date of access: 20 Jan. 2020.

DCAF. 2017. Backgrounders Series: Intelligence Oversight. backgrounders@dcaf.ch Date of access: 20 Jan. 2020.

BIBLIOGRAPHY

De Lima Silva, D.F., Silva, J.C.S., Silva, L.G.O., Ferreira, L. and de Almeida-Filho, A.T., 2018. Sovereign Credit Risk Assessment with Multiple Criteria Using an Outranking Method, Hindawi, *Mathematical Problems in Engineering*, Vol: (2018):1-11. https://doi.org/10.1155/2018/8564764 Date of access: 18 Nov. 2021.

Der Derian, J. 1992. Antidiplomacy: Spies, terror, speed, and war. Oxford: Blackwell.

DeRouen J.R.K and Goldfinch, S. 2013. What Makes a State Stable and Peaceful? Good Governance, Legitimacy and Legal-Rationality Matter Even More for Low-Income Countries. London: Taylor & Francis. http://dx.doi.org/10.1080/13698249.2012.740201 **Date of access: 13 Aug. 2022.**

Dokken, K, 2001. African Security Politics Redefined. New York, NY: Palgrave Macmillan.

Doumpos, M. and Zopounidis, C. 2002. Multicriteria Decision Aid Classification Methods. New York, NY: Kluwer Academic Publishers, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.570.318&rep=rep1&type=pdf. Date of access: 04 Dec. 2021.

ESI Africa, 2022. World Bank: SA's energy transition can be both just AND climate resilient. https://www.esi-africa.com/news/world-bank-sas-energy-transition-can-be-both-just-and-climate-resilient/ Date of access: 2 Nov. 2022.

Etymology Dictionary Online, Harper, D. (2001-2022). https://www.etymonline.com/ Date of access: 15 Aug. 2021.

Expert Panel **see** South Africa.

Fingar, T. 2011. Reducing Uncertainty - Intelligence Analysis and National Security. California, CA: Stanford University Press.

Foucault, M.1991. Security, Territory, Population. Lectures at the College de France, 1977 – 1978. http://tems.umn.edu/Foucault,%20Governmentality.pdf Date of access: 2 Jan. 2019.

Fukuyama, F. 2013. Public Lecture by Dr Francis Fukuyama, Linder Auditorium, 10 May 2013. http://www.mistra.org.za/Media/Speeches/Pages/The-Origins-of-Political-Order-by-Francis, Date assess: 19 Feb. 2015.

BIBLIOGRAPHY

General Intelligence Law Amendment **see** South Africa.

General Intelligence Laws Amendment (GILAA) **see** South Africa.

Geneva Centre for the Democratic Control of Armed Forces, 2017. 'Intelligence Services', SSR Backgrounder Series, Geneva: DCAF.

Gill, P. 2009. Theories of intelligence: Where we are, where should we go and how might we proceed? (In Gill, P., Marrin, S. and Phythian, M. eds. 2009: Intelligence Theory: Key questions and debates. Studies in Intelligence). London: Routledge, pp. 208-226.

Gill, P., Marrin, S. and Phythian, M. eds. 2009. Intelligence Theory: Key questions and debates, London: Taylor & Francis Ltd.

Gill, P. and Phythian, M. 2006. Intelligence in an insecure world, first ed. Cambridge: Polity Press.

Gill, P. and Phythian, M. 2012. Intelligence in an insecure world, 3rd ed. Cambridge: Polity Press.

Gill P. 2012. Intelligence, Threat, Risk and the Challenge of Oversight. Journal: Intelligence and National Security 27(2):206–222.

Gill P,& Phythian M. 2018. Intelligence in an Insecure World. 3th edition. Cambridge: Polity Press.

Godson, R., *ed*. 1983. Intelligence requirements for the 1980s. Washington, D.C.: National Strategic Information Centre.

Government Gazette **see** South Africa.

Handel, MI. 1977: The Yom Kippur War and the Inevitability of Surprise. *International Studies Quarterly*, 21(3):461-502 http://www.jstor.org/stable/2600234 Date of access: 16 Jan. 2020.

Hannah, G, O'Brien, K.A. and Rathmell, A. 2005. Intelligence and Security Legislation for Security Sector Reform. Santa Monica, CA: RAND Corporation.

Herman, M. 1996. Intelligence Power in Peace and War. 5th edition. Cambridge: Cambridge University Press, England.

BIBLIOGRAPHY

Heuer, RJ. Jnr. 1999: Psychology of Intelligence Analysis. Centre for the Study of Intelligence, Central Intelligence Agency, USA

Heuer, R.J. and Pherson, R.H. 2011. Structured analytical techniques for intelligence analysis. Washington, DC: CQ Press.

High-Level Review Panel (HLRP) **see** South Africa.

Hilsman, R. 1952. Intelligence and Policymaking in Foreign Affairs. *World Politics*, 5(1):1–45. https://doi.org/10.2307/2009086 Date of access: 3 Apr. 2018

Honig O.A. 2007. A new direction for theory-building in intelligence studies. *International Journal of Intelligence and Counter Intelligence*, 20(4): 699–716,. Taylor & Francis Group, LLC.

Oxford Advanced Learner's Dictionary. 2013. (Eds. Hornby A.S., Turnbull J., Lea D., Parkinson D. and Phillips P. 8th edition (OALD). Publisher**:** Oxford: Oxford University Press.

Hough M. 2006. The Concept of a National Security Strategy: The case of the United States and South Africa. https://repository.up.ac.za/handle/2263/3079 Date of access: 17 Nov. 2017.

Hough, P. 2013. Understanding Global Security, 2nd edition. Oxon, OX: Routledge.

Hulnich, A.S. 2005. Indications and Warning for Homeland Security: Seeking a New Paradigm. *International Journal of Intelligence and Counterintelligence.* 18(4):593-608 http://www.tandfonline.com/loi/fint20 Date of access: 04 Nov. 2018.

Hulnich, A.S. 2006. What's wrong with the Intelligence Cycle, *International Journal Intelligence and National. 21(6):959-979* http://www.tandfonline.com/loi/fint20 Date of access: 04 Nov. 2018.

Human Rights Watch, Website (2021). World Report, South Africa 2020 https://www.hrw.org/world-report/2021/country-chapters/south-africa Date of access: 13 Sep. 2023.

Hurwitz, L. 1973. Contemporary Approaches to Political Stability. Source: Comparative Politics, 5(3):449-463. http://www.jstor.org/stable/421273?origin=JSTOR-pdf Date of access: 1 Aug. 2022.

BIBLIOGRAPHY

International Monetary Fund (IMF): Country Report: South Africa, 2006-2020: https://www.imf.org/en/Countries/ZAF Date of access: 20 Jun. 2022.

International Convergence of Capital Measurement and Capital Standards. 2011. BS 31100: *The British Code of Practice for Risk Management & Guidance for ISO31000. London*: British Standards Institute

Intelligence Services Control Act **see** South Africa.

Intelligence Services Act **see** South Africa.

Investopedia, Kenton, W. 2022. Define Economy. https://www.investopedia.com/terms/e/economy.asp Date of access: 04 Aug. 2022.

IOL media. 14 Jul. 2021 Poverty and hunger a ticking time bomb, says Abahlali base Mjondolo. https://www.iol.co.za/news/politics/poverty-and-hunger-a-ticking-time-bomb-says-abahlali-basemjondolo-e8557dda-ea3e-4fc1-9a71-747982baf17c Date of access: 31 Oct. 2022.

ISO 31000: 2009, International Organization for Standardization (ISO) Geneva: Central Secretariat.

ISO/IEC Guide 73/2009, International Organization for Standardization (ISO) Geneva: Central Secretariat.

IWGNS. 2013. 'International Working Group on National Security. http://www.ssronline.org/national_security_index.cfm Date of access: 24 Jul. 2016.

Johnson, R. 1999. Post-Cold War security: the lost opportunities. https://unidir.org/files/publications/pdfs/the-new-security-debate-en-364.pdf .Date of assess: 04 Nov.2018

Johnson, L.K. 2003. Preface to a Theory of Strategic Intelligence, *International Journal of Intelligence and Counterintelligence*, 16(4): 638–663, DOI; Taylor & Francis Inc. https://www.tandfonline.com/doi/abs/10.1080/716100470 Date of access: 6 Jun. 2017

Johnson, L.K. 2009. Handbook of Intelligence Studies. New York, NY: Routledge.

BIBLIOGRAPHY

Kahneman D. 2011. Thinking, Fast and Slow. London: Penguin Books London

Kahneman, D. and Tversky. A. 1979. Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, 47(2):263-291. Econometric Society Stable http://www.jstor.org/stable/1914185 Date of access: 04 Apr. 2019.

Kahn, D. 2001. An historic theory of intelligence. Journal of Intelligence and National Security, 16(3):79-92.

Kaplan, R.S. and Mikes, A. 2012. Managing Risks: A New Framework. Havard Business Review https://hbr.org/2012/06/managing-risks-a-new-framework Date of access: 04 Jan. 2019.

Kaufmann, D., and Kraay A. 2022: Governance Indicators: Where Are We, Where Should We Be Going? World Bank http://info.worldbank.org/governance/wgi/pdf/wps4370.pdf Date of access: Sep. 2022.

Keat, P. 2008. What markets miss: political stability frameworks and country risk. (In Bracken, P. Bremmer, I. and Gordon, D. 2008: Managing Strategic Surprise (Lessons from Risk Management and Risk Assessment). London: Cambridge University Press. pp. 265-286.

Kent, S. 1953. Strategic intelligence for American world policy. London: Oxford University Press.

Kent, S. 1966. Strategic intelligence for American world policy. Princeton: Princeton University Press.

Kent, S. 1955. The Need for an intelligence literature. Studies in Intelligence, https://www.cia.gov/library/center-for-the-study-of-intelligence Date of access: 19 Aug. 2015.

Keynes, J.M., 1936. The General Theory of Employment, Interest and Money. ETN Zurich: International Relation, and Security Network. https://www.files.ethz.ch/isn/125515/1366_KeynesTheoryofEmployment.pdf Date of access: 26 Sep. 2019.

King Report (I – IV): 1994 (King I), 2002 (King II), 2009 (King III) and 2016 (King IV). King Report on Corporate Governance. Institute of Directors in Southern Africa (IoDSA). https://www.iodsa.co.za/page/king_iv_report Date of access: 10 Apr. 2017.

BIBLIOGRAPHY

Kirkpatrick, Jr. and Lyman B. 1969. Captains Without Eyes: Intelligence Failures in World War II. London: MacMillan Company.

Kloman, HF. 2010. A Brief History of Risk Management. (*In* Fraser, J. and Simkins, B.J. Enterprise Risk Management, The Robert W. Kolb Series in Finance). New Jersey: John Wiley & Sons, Inc.

Knight, F. 1921. Risk, Uncertainty and Profit. New York: Dover Publication, Inc.

Koetje F, 1999. South African national security policy: An international relations perspective. *African Security Review*, 8(6): pp. 44-57 https://www.tandfonline.com/doi/pdf/10.1080/10246029.1999.9628159 Date of access: 26 Sep. 2019.

Koschade, S. 2006. A Social Network Analysis of Jemaah Islamiyah: The Applications to Counterterrorism and Intelligence. Studies in Conflict and Terrorism 29(6):559-575. https://www.researchgate.net/publication/45588571_Social_Network_Analysis_in_the_Study_of_Terrorism_and_Political_Violence Date of access: 8 May 2017.

Lahneman, W.J. 2010. The need for a new intelligence paradigm. *International Journal of Intelligence and Counterintelligence*, 23(2):201–225.

Lowenthal, M. 2009. Intelligence: from secrets to policy. 4th ed. Washington DC: CQ Press.

Louisot, J. and Ketcham, C.H. 2014. Enterprise Risk Management, Issues and Cases. West Sussex: John Wiley & Sons Ltd.

Lundquist, L., 1993. Det vetenskapliga studiet av politik, Lund: Studentlitteratur

Mabey, N., Gulledge, J. Finel B. & Silverthorne K. (February 2011) Degrees of Risk (Defining a Risk Management Framework for Climate Security) Washington DC, Attribution-Non-commercial –Share

MacEachin, D. 2002. Predicting the Soviet Invasion of Afghanistan: *The Intelligence Community's Record*. McLean, VA: Central Intelligence Agency, Centre for the Study of Intelligence. http://www.cia.gov/cs Date of access: 20 Feb. 2017.

BIBLIOGRAPHY

Machiavelli, N. (1532 repr. n.d.) *The Prince.* http://www.constitution.org/ mac/prince06.htm. Date of access: 04 Feb. 2016.

Mail and Guardian, Rodrigues, C., 5 April 2010. 'Black Boers' and Other Revolutionary Songs. https://thoughtleader.co.za/on-revolutionary-songs/ Date of access: 31 Oct. 2022.

Mail and Guardian, Sapa-AFP. 8 Jan 2014. Zuma: The ANC Will Rule till Jesus Comes Back. https://mg.co.za/article/2014-01-08-zuma-the-anc-will-rule-forever/ Date of access: 14 Oct. 2022.

Maree, K. 2007. First steps in research. Pretoria: Van Schaik Publishers.

Masetlha v President of the Republic of South Africa and Another, 2008 (1) SA 566 (CC) http://www.saflii.org/za/cases/ZACC/2007/20.html Date of access: 20 Jul. 2022.

McCarthy, M. 1994. The National Warning System: Striving for an Elusive Goal, *Defense Intelligence Journal* 3(1): 5-19.

Minister Godongwana: Medium Term Budget Policy Statement **see** South Africa.

Ministerial Review Commission on Intelligence **see** South Africa.

National Commission on Terrorist Attacks Upon the United States, public report released on July 22, 2004; http://www.9-11commission.gov Date of access: 3 Jul. 2017.

National Treasury. 2022. South Africa Government. https://oag.treasury.gov.za/Guidelines/Forms/AllItems.aspx Date of access: 20 Jun. 2022.

Neethling, T. 2012. Revisiting South Africa's Contemporary Political Risk Profile. *Southern African Peace and Security Studies*, 2 (1): 35-58 http://www.saccps.org/pdf/2-1/Neethling%20(article).pdf Date of access: 21 Jun. 2022.

Neethling, T. 2016. An update on South Africa's political risk profile in 2015/6. New Contree, No. 75. http://dspace.nwu.ac.za/bitstream/handle/10394/19408/No_75_%282016%29_4_%20Neethling.pdf?sequence=1&isAllowed=y Date of access: 25 Jun. 2022.

BIBLIOGRAPHY

Neethling, T. 2021. South Africa's political risk profile has gone up a few notches: but it's not yet a failed state. *The Conversation*. https://theconversation.com/south-africas-political-risk-profile-has-gone-up-a-few-notches-but-its-not-yet-a-failed-state-170653 Date of access: 20 Jun. 2022.

News 24, Cowan, K. 12 May 2022. Spy Agency Boss Cracks the Whip: Staff Warned to Comply with Forensic Investigators or Face Action. https://www.news24.com/news24/investigations/spy-agency-boss-cracks-the-whip-staff-warned-to-comply-with-forensic-investigators-or-face-action-20220512-2 Date of access: 3 Aug. 2022.

News 24, Gerber, J. 02 Aug 2021. Unrest SA: DA wants transparent, credible parliamentary inquiry. https://www.news24.com/news24/southafrica/news/unrestsa-da-wants-transparent-credible-parliamentary-inquiry-20210802 Date of access: 3 Aug. 2022.

News 24, Patrick, A. 27 October 2022. Rand Water chief says areas supplied by the utility won't experience 'Day Zero' scenario. https://www.news24.com/news24/southafrica/news/live-rand-water-implements-stage-2-supply-restrictions-20221021 Date of access: 27 Oct. 2022.

News 24, Patrick, A. 27 October 2022. Water 'crisis' meeting: Scientist says Joburg consumption is below global use, not a factor in shedding. https://www.news24.com/news24/southafrica/news/water-crisis-meeting-scientist-says-joburg-consumption-is-below-global-use-not-a-factor-in-shedding-20221027 Date of access: 27 Oct. 2022.

Nhamo, L. (2022), New agricultural pathways key for food security. *Food For Mzansi.* https://www.foodformzansi.co.za/new-agricultural-pathways-key-for-food-security/ Date of access: 31 Oct. 2022.

New York Times, 2013. Andrew Ross Sorkin, A.R. How Mandela Shifted Views on Freedom of Markets. https://dealbook.nytimes.com/2013/12/09/how-mandela-shifted-views-on-freedom-of-markets/ Date of access 2 Oct. 2022.

O'Brien, K. 2011. The South African Intelligence Services: From Apartheid to Democracy 1948-2005. Abington: Routledge.

OECD (2015), G20/OECD Principles of Corporate Governance. Paris: OECD Publishing. http://dx.doi.org/10.1787/9789264236882-en Date of access: 2 Aug. 2022.

BIBLIOGRAPHY

Ostrom, E., 2007. Background on the Institutional Analysis and Development Framework. *The Policy Studies Journal*, 39(1). Oxford: Wiley Periodicals, Inc.

Oxford English Dictionary (1989). Clarendon: Oxford University Press.

Pace, C. 2018. The Threat Intelligence Handbook- A Practical Guide for Security Teams to Unlocking the Power of Intelligence. Parkway, MD: CyberEdge Group.

Parker, C.F. 2007. Warning for Readiness in the New Threat Environment. Workshop Report, *Global Futures Forum: Emerging Threats in the 21st Century*, Seminar 3. Zurich: Centre for Security Studies. http://www.crn.ethz.ch/publications/crn_team/detail.cfm?lng=en&id=47345 Date of access: 11 Nov. 2014.

Parliament of South Africa. 2021. Annual Report of the Joint Standing Committee on Intelligence (JSCI) for the. Financial Year ending 31 March 2020, including the period to December 2020. Cape Town. www.parliament.gov.za Date of access: 4 Jul. 2022.

Pauw, J. 2017: The President's Keepers. Those Keeping Zuma in Power and Out of Prison. Cape Town: Tafelberg.

Phakathi, B. 2020. SA Records Sharp Drop in Foreign Direct Investment. Available online https://www.businesslive.co.za/bd/economy/2020-06-17-sa-records-sharp-drop-in-foreign-direct-investment/ Date of access: 10 Oct. 2021.

Phythian, M. 2009. Intelligence theory and theories of international relations: shared world or separate worlds. Page: 54-72. (*In* Gill, P., Marrin, S. & Phythian, M., eds.) Intelligence theory. Key questions and debates. New York: Routledge.

Pew Research Centre, 2019, In South Africa, racial divisions and pessimism about democracy loom over elections. https://www.pewresearch.org/fact-tank/2019/05/03/in-south-africa-racial-divisions-and-pessimism-over-democracy-loom-over-elections/ Date of access: 03 Nov. 2022.

Planning Commission **see** South Africa.

Protection of Information Act **see** South Africa.

BIBLIOGRAPHY

Public Finance Management Act **see** South Africa.

Pye, L. W.; and Verba, S. 1965 Political Culture and Political Development. Princeton: Princeton University Press

The Public Service Regulations **see** South Africa.

Treverton, G.F.; Jones, S.G.; Boraz, S. and Lipscy, P. 2009. RAND Conference 2006: Towards a theory of intelligence. First published 2009, Abingdon: Routledge. https://www.rand.org/content/dam/rand/pubs/conf_proceedings/2006/RAND_CF219.pdf Date of access: 06 Nov. 2016.

Rand Daily Mail, 31 October 2016 Cost of #FeesMustFall now R1bn, says universities official. https://www.businesslive.co.za/archive/2016-10-31-cost-of-feesmustfall-now-r1bn-says-universities-official2/ Date of access: 24 Nov. 2022.

Ratcliffe, H.J. 2008. Intelligence-Led Policing. Devon: Willan Publishing.j

Rathmell, A. 2002. Towards postmodern intelligence. *Journal, Intelligence and National Security* 17(3):87-104, New York: Routledge.

Regulation of Interception of Communication and Provision of Communication Related Information Act **see** South Africa.

Ritzer, G. 2001: Explorations in Social Theory - From Metatheorizing to Rationalization. California: SAGE Publications Inc.

Sabatier, P.A. 2007. Theories of the Policy Process. Colorado: Westview Press.
Schwartz, P. 1996: The art of the long view: paths to strategic insight for yourself and your company. New York: Bantam Doubleday Dell Publishing Group, Inc.

Schwella, E. *et al.* 2017. South African Governance. Cape Town: Oxford University Press.

Scott, L. 2004. Secret intelligence, covert action, and clandestine diplomacy. Journal, *Intelligence and National Security,* 19(2): 322-341. New York: Routledge.

BIBLIOGRAPHY

Scott, L. 2007. Sources and methods in the study of intelligence: A British view. (*In* Johnson, L.K. *ed.* 2007. Strategic intelligence: Understanding the hidden hand of government. Westport, CT: Praeger Security International. p. 89-108.

Scott, L. & Jackson, P. 2004. The Study of Intelligence in Theory and Practice. *Journal: Intelligence and National Security*, 19(2):139-169. https://doi.org/10.1080/0268452042000302930 Date of access: 18 Nov. 2018.

Sheehan, M. ed. 2000. National and international security. Burlington: Ashgate Publishing Company.

Shiels, F.L., 1991. *Preventable Disasters:* Why Governments Fail. Savage, MD: Rowman and Littlefield Publishers.

Shulsky, A. and Schmitt, G. 2002. Silent warfare: understanding the world of intelligence. Dulles: Potomac Books.

Silberman-Robb, 2005. Report: United States Regarding Weapons of Mass Destruction, https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/WMDCommissionReport.pdf Date of access: 3 Jan. 2022.

Sims, JE. 2009. Defending Adaptive Realism. In Intelligence Theory: Key questions and debates. London: Routledge, pp. 151-165.

Sims, J.E.. 2005. Understanding Friends and Enemies: The Context for American Intelligence Reform. Washington, D.C.: Georgetown University Press. pp. 14-31.

Siu, Y.L. 2009. A Meta-Theory of Risk: Risk as Reflexive, Social Learning. *Sustainability Research Institute School of Earth & Environment University of Leeds*. SCARR International Conference, 15th – 17th April 2009. Beijing: Normal University.

Skeat W.W. 1880. English language - Etymology Dictionary. Toronto: Oxford Clarendon Press. https://archive.org/details/etymologicaldict00skeauoft Date of access: 5 Febr. 2018

Skjong R. 2005. internet webpage, *research.dnv.com/skj/*Study*s/etymology-of-risk.pdf* Date of access: 5 Aug. 2016.

BIBLIOGRAPHY

South Africa. 1996. Constitution of the Republic of South Africa Act 108 of 1996**.** Pretoria: Government Printer.

South Africa. 2002a. Electronic Communications and Transactions Act 25 of 2002. Pretoria: Government Printer

South Africa, 2021. Expert Panel: Report of The Expert Panel into The July 2021 Civil Unrest. Pretoria: Presidency https://www.thepresidency.gov.za/content/report-expert-panel-july-2021-civil-unrest Date of access: 20 Jan. 2022.

South Africa. 2000. General Intelligence Law Amendment Act 66 of 2000. Pretoria: Government Printer.

South Africa. 2013. General Intelligence Laws Amendment Act No 11 of 2013 (GILAA). Pretoria: Government Printer.

South Africa, 2020. Government Gazette, Proclamation No13 of 2020. Establishment of the National Security Council. Pretoria: Government Printer.

South Africa, High-Level Review Panel into the State Security Agency. South Africa, December 2018. https://www.politicsweb.co.za/documents/report-of-the-highlevel-review-panel-on-the-ssa Date of access: 08 Jan. 2019.

South African Institute of Race Relations (IRR). 2016. Life in South Africa: Reasons for Hope. Johannesburg: The South African Institute of Race Relations, https://irr.org.za/reports/occasional-reports/files/life-in-south-africa-reasons-for-hope.pdf Date of access: 20 Jul. 2022.

South Africa. 1999. Intelligence Services Control Act into an amendment Act 42 of 1999. Pretoria: Government Printer.

South Africa. 2002b. Intelligence Services Act 65 of 2002. Pretoria: Government Printer.

South Africa. 26 October 2022. Minister Godongwana: Medium Term Budget Policy Statement. Government Website: https://www.gov.za/speeches/minister-enoch-godongwana-medium-term-budget-policy-statement-26-oct-2022-0000 Date of access: 27 Oct. 2022.

BIBLIOGRAPHY

South Africa. Ministerial Review Commission on Intelligence. 10 September 2008. Pretoria: The Minister of Intelligence. https://www.r2k.org.za/wp-content/uploads/Matthews-Commission-Report-10-Sept-2008.doc Date of access: 20 Oct. 2016.

South Africa Planning Commission: Report of 19 October 2018: Measurement of Progress with the Implementation of the National Development Plan (NDP): A Six-Year Analysis. Pretoria: National Planning Commission.

South Africa. 1984. Protection of Information Act No 82 of 84. Pretoria: Government Printer.

South Africa. 1999. Public Finance Management Act No 1 of 1999. Pretoria: Government Printer.

South Africa. 2016. The Public Service Regulations (Issued in 2016). Pretoria: Government Printer.

South African Reconciliation Barometer. 2021. Institute for Justice and Reconciliation, www.ijr.org.za. Produced by COMPRESS.dsl https://www.ijr.org.za/portfolio-items/south-african-reconciliation-barometers-survey-2021-report/ Date of access: 12 Sep. 2022.

South Africa. 2002. Regulation of Interception of Communication and Provision of Communication Related Information Act 70 of 2002. Pretoria: Government Printer.

South Africa, State Security Agency (SSA) Website, http://www.ssa.gov.za/ (Date of access: 07 October 2020)

South Africa. Statistics South Africa Website: (Date of access: 04 November 2022) https://www.statssa.gov.za/?p=15407

South Africa. The Treasury Regulations as amended (Issued in 2001). Pretoria: Government Printer.

South Africa. 2002c. The Intelligence Services Control Amendment Act 66 of 2002. Pretoria: Government Printer.

South Africa. 1994. The Intelligence Services Oversight Act 40 of 1994, Pretoria: Government Printer.

South Africa. 2002. The Intelligence Services Act 65 of 2002, Pretoria: Government Printer.

BIBLIOGRAPHY

South Africa. 1994. The National Strategic Intelligence Act 39 of 1994, Pretoria: Government Printer.

South Africa. 2002d. National Strategic Intelligence Amendment Act 67 of 2002. Pretoria: Government Printer

South Africa. 1994. The Public Service Act 103 of 1994, Pretoria: Government Printer.

South Africa. 2016. The Public Service Regulations (Issued in 2016), Pretoria: Government Printer.

South Africa. 2001. The Treasury Regulations as amended (Issued in 2001), Pretoria: Government Printer.

South Africa. 1994. White Paper on Intelligence. http://www.info.gov.za/white*papers*/1995/intelligence.htm or http://www.nia.gov.za/SSA-web-Legislation%20and%20Oversight.html. Date of access: 05 Oct. 2014.

Southern African Peace and Security Studies (SAPSS) 2014. Neethling, T. Revisiting South Africa's Contemporary Political Risk Profile. *Published by the Southern African Centre for Collaboration on Peace and Security (SACCPS)*, 2(1). www.saccps.org Date of access: 27 Jun. 2022.

State Security Agency **see** South Africa.

Statistics South Africa (Stats SA 2021). Economic Growth. https://www.statssa.gov.za/?page_id=735&id=1 Date of access: 2 Aug. 2022.

Statistics South Africa (Stats SA 2018). BRICS Joint Statistical Publication 2018. Pretoria: Statistics South Africa. https://www.statssa.gov.za/?page_id=735&id=1 Date of access: 2 Aug. 2022.

Stern, J. and Wiener, J. B. 2006: Precaution against Terrorism. *Journal of Risk Research* 9(4):393–447. New York: Routledge, https://study.com/ Date of access: 26 Jul. 2022.

Sunday Times, Insight. Shaw, M. and Rademeyer, J., 25 September 2022. The Dark Tangled Web Strangling SA. Pp.13-14. https://www.timeslive.co.za/sunday-times/opinion-and-analysis/insight/2022-09-25-the-dark-tangled-web-strangling-sa/ Date of access: 30 Sep. 2022.

Sun Tzu. 2005. The Art of War. (Translated by Cleary T.). Boston and London: Shambhala.

BIBLIOGRAPHY

Sun Tzu, 1963. The Art of War. (Translated by Samuel B. G.). Oxford: Oxford University Press.

The Cadbury Report, 1992. The Financial Aspects of Corporate Governance. London: Gee (a division of Professional Publishing Ltd).

The Treasury Regulations **see** South Africa.

The Intelligence Services Control Amendment Act **see** South Africa.

The Intelligence Services Oversight Act **see** South Africa.

The Intelligence Services Act **see** South Africa.

The Public Service Act **see** South Africa.

The Public Service Regulations **see** South Africa.

The Treasury Regulations **see** South Africa.

The 9/11 Commission Report, July 2004. Final Report of the National Commission on Terrorist Attacks Upon the United States. Washington: Government Printing Office. https://www.govinfo.gov/content/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf Date of access: 7 Aug.2017.

The Ibrahim Index of African Governance (IIAG), 2022, South Africa Data http://www.moibrahimfoundation.org Date of access: 4 Apr. 2022.

The Oxford Advanced Learner's Dictionary, 8th edition (OALD) (2010), Oxford: Oxford University Press.

The Oxford Dictionary (1984) and Concise Oxford Dictionary (1999), Oxford**:** Oxford University Press.

The New York Times, Sorkin, A.R. December 9, 2013: How Mandela Shifted Views on Freedom of Markets. https://dealbook.nytimes.com/2013/12/09/how-mandela-shifted-views-on-freedom-of-markets/ Date of access: 20 Oct. 2022.

BIBLIOGRAPHY

Tilman L.M. 2013. Risk Intelligence: A Bedrock of Dynamism and Lasting Value Creation Money & Wealth. Risk IntelligenceTwitterFacebookLinkedInGoogle+ PinterestLineViberWhatsAppWeChat. Date of access: 7 Feb. 2019.

Transparency International Corruption Index (TICI), 2022. Johannesburg: Corruption Watch. https://www.transparency.org/en/countries/south-africa Date of access: 3 Oct. 2022.

Treverton, G.F. 2003. Reshaping National Intelligence for an Age of Information. Cambridge: Cambridge University Press.

Troy, T.F. 2008. The 'correct' definition of intelligence. *International Journal of Intelligence and Counterintelligence*, 5(4):433-454. London: Routledge. http://www.tandfonline.com/loi/ujic20. Date of access: 17 Nov. 2018.

Tversky A. and Kahneman, D. 1973. A Heuristic for Judging Frequency and Probability. *Cognitive Psychology*: 5:207-232 (1973). Oregon Research Institute: The Hebrew University of Jerusalem Date of access: 21 Oct. 2018.

United Cities and Local Governments Asia-Pacific, 2021. Indonesia. https://uclg-aspac.org/good-governance-definition-and-characteristics/ (Date of access: 7 Jul. 2022.

United Nations. 2022. Stainable Stock Exchange Initiative. Website, https://sseinitiative.org/stock-exchange/jse/#:~:text=About%20the%20stock%20exchange&text=The%20JSE%20is%20currently%20ranked,exchange%20in%20the%20African%20continent. Date of access: 20 Oct. 2022.

Unit Nations. 2022. Development Programme (UNDP). Human Development Report 2021/22. https://hdr.undp.org/system/files/documents/global-report-document/hdr2021-22pdf_1.pdf Date of access: 3 Oct. 2022.

Unit Nations 2012. System Task Team, Governance and development online. https://www.un.org/millenniumgoals/pdf/Think_Pieces/7_governance.pdf Date of access: 23 Sep. 2022.

US News and World Report. 2022/23. Best Universities ranging in Africa. https://www.usnews.com/education/best-global-universities/africa Date of access: 20 Sep. 2022.

BIBLIOGRAPHY

Valsamakis, A.C., Vivian, R.W., and Du Toit, G.S. 2005. Risk Management, Managing Enterprise Risks. 3rd. ed Sandton, Heinemann Publishers.

Van Den Berg, M.A. 2014. Intelligence regimes in South Africa (1994–2014): and analytical perspective. Potchefstroom: North-West University. (Thesis – Masters).

Van Den Berg, M.A. 2018. Intelligence practices in South Africa as hybrid political regime: a meta-theoretical and theoretical analysis. Potchefstroom: North-West Univeristy. (Thesis – PhD).

Van der Heijden, K. 2005. The Art of Strategic Conversation, 2nd ed. West Sussex: John Wiley & Sons Ltd.

Walsh, P.F., 2011**.** Intelligence and intelligence analysis, 4th ed. New York: Routledge.

Walsh, P.F. 2014. Building better intelligence frameworks through effective governance - *International Journal Intelligence and National Security 28(1):123-142* London: Routledge. http://www.tandfonline.com/loi/fint20 Date of access: 02 Sep. 2015.

Warner, M. 2009. Intelligence as risk-shifting. (In Gill, P., Marrin, S. and Phythian, M. eds. Intelligence theory. Key questions and debates). New York: Routledge. Pages: 16-32.

Wheaton, K.J. and Beerbower, M.T. 2006. Towards a definition of intelligence. *Stanford Law & Policy Review*, 17(2): 319-331.

White Paper **see** South Africa.

Wirtz, J.J. 1991. The Tet Offensive: Intelligence Failure in War. Ithaca, NY: Cornell University Press.

Wohlstetter, R. 1962. Pearl Harbor: Warning and Decision. Palo Alto, CA: Stanford University Press.

World Bank, 2018. South Africa Economic Update - Jobs and Inequality. Washington, DC: The World Bank. https://pubdocs.worldbank.org/en/798731523331698204/South-Africa-Economic-Update-April-2018.pdf Date of access: 20 Sep. 2022.

World Bank, 2022. Esi-africa - World Bank: SA's Energy Transition Can Be Both Just and Climate Resilient. https://www.esi-africa.com/tag/world-bank/ Date of access: 3 Nov. 2022.

BIBLIOGRAPHY

World Economic Forum (WEF), 2022. World Risk Report 2022. https://www.weforum.org/reports/global-risks-report-2022/ Date of access: 1 Nov. 2022.

Young, J. 2008. Operational Risk Management (The Practical Application of a Qualitative Approach). 3rd ed. Pretoria: Van Schaik Publishers.

Zinn, J.O. 2008. Social Theories of Risk and Uncertainty. Oxford: Blackwell Publishing Ltd.