UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Gordon Institute of Business Science
University of Pretoria

Enterprise Risk Management within public sector institutions for improving compliance: A case study into a public sector institution

Boitumelo Mokgatle

12328228

A research project submitted to the Gordon Institute of Business Science, University of Pretoria, in partial fulfilment of the requirements for the degree of Master of Business Administration.

11 November 2013

ABSTRACT

Performance of the institutions in the public sector has always been among the main drivers that determine how the country is ultimately perceived by its citizens and the world, it is the policies and regulations established by these institutions that governs the private sector. The objectives of these public institutions can only be achieved through well formulated, well implemented and a continuous review of the strategies being pursued to achieve the stated objectives. At the core of setting strategies is Enterprise Risk Management (ERM), being an organisational procedure enabling the identification, assessment and action plans for the organisational risks linking to the achievement of objectives. The action plans formulated through the ERM should translate into strategic objectives mainly in the public sector where resources are chronically limited. Even with good intentions, government may spend badly because it has either chosen the wrong projects to fund or planned badly for good projects if the strategies are not continually and systematically reviewed.

The objective of this research was to gain an understanding of how risk management is conducted at an enterprise-wide level within public sector institutions to ensure that the institution complies with all the relevant requirements within its ambit. It was a qualitative study that was conducted using a case study methodology wherein a public sector institution was identified and the executives involved in the risk management were interviewed individually. Semi-structured interviews were conducted and the results were analysed through the themes that were identified.

The study identified that more understanding is required by public sector organisations to be able to realise the benefits of ERM. A clear distinction of what the objectives of the institution are, the related strategies, strategic objectives and risks to the strategic objectives, need to be made clear. The use of risk registers at different levels of the organisation is a tool to draw the relevant risks from deep in operations to a strategic level and this has to be understood at all levels. More importantly the correct action plans in reaction to identified risks can greatly turn risks into opportunities but this is not currently the case as risk registers are still not well implemented and utilized. Risk identification should not be a brainstorming session when the strategy is created but a continuous well operated system within operations throughout the period. The risk culture, roles and relevant systems are still lacking in public institutions.

KEYWORDS

Enterprise Risk Management

Strategic Risk

Public Sector

Regulatory Institutions

Enforcement

Compliance

DECLARATION

I declare that this research project is my own work. It is submitted in partial fulfilment of the requirements for the degree of Master of Business Administration at the Gordon Institute of Business Science, University of Pretoria. It has not been submitted before for any degree or examination in any other University. I further declare that I have obtained the necessary authorisation and consent to carry out this research.

Boitumelo Mokgatle

11 November 2013

DEDICATION

I dedicate this research to my husband, my two sons and my home-keeper.

Danny you have been a mom and dad to our boys while I just simply could not be there and I will forever be grateful.

To my dearest treasures my sons Risizi and Risima who still loved their mommy unconditionally regardless of all the long hours they had no idea where she was, this is for you boys from mommy with all my love.

To my ever-so-humble house keeper and home-maker Stella, I will forever respect you for giving my home your consistent attention for years. I always could go home to the same smell and touch of a happy home.

ACKNOWLEDGEMENTS

Thank you to all the 2012/2013 MBA class that I am now a much better person from all the knowledge you shared in and out of class, it has been a blissful journey indeed.

A special thank you to the “Colombians” for the long hours preparing for exams and sharing information as much as possible, this experience would not have been the same without you.

To Jabu my supervisor for all the assistance and feedback, a sincere thank you. Your commitment to assist me by whatever means possible was my inspiration.

To my employer South African Revenue Service (SARS), I am grateful for the financial assistance and the time away from work that I was given.

To my family, I will be forever indebted to you.

To the public institution that opened its doors and was a subject of my research, the CEO, all the officials that took time off their busy schedules to participate in this research, I will forever be grateful.

Last but not least, I would like to thank The Almighty for all that I am, all that I have been, and all that I will be.

TABLE OF CONTENTS

1 CHAPTER ONE: DEFINITION OF PROBLEM AND PURPOSE

1.1 Why was this problem selected

Globally, organisations are increasingly applying a “risk lens” to their businesses. This creates an advantage through more efficient deployment of scarce resources, better decision-making and reduced exposure to negative events (Ernst & Young, 2012). Public sector organisations are not any different in this requisite for a systematic risk management methodology relating to their stated strategic objectives. Examining public sector risk management is an opportunity for researchers as well as the universities, as better understanding and management of strategic risk can lead to more effective strategy development and planning, ultimately leading to better communities and provinces (Cooper, 2010, p. 5).

For any organisation whether for profit or not, to achieve its stated objectives it has to have a strategy. Therefore the strategy as stated above, comes with the responsibility of identifying all possible related risks together with mitigation plans related to the risks. This then calls for the co-existence of strategic risk management as an unavoidable part of setting strategies; furthermore it must be noted that without risks, gains are unlikely (Coetzee & Lubbe, 2013).

The high rate of collapses by some reputable businesses around the world exemplified by events at Worldcom Inc., Enron Corp., and others, helped shape a desire for an integrated view of risk, as audit committees, executives and boards were receiving conflicting information (Muzzy, 2008), and coupled with scandals of fraud over the past years has led to senior managers being expected to now comply with laws and regulations whereby corporate governance and risk management is actively monitored (Ballou & Heitger, 2005).

This has led to the incorporation of risk committees being currently required by the different guidelines as per the likes of the South African King III report (King, 2009) the Australian corporate governance principles and recommendations (Council & Exchange, 2007), the Belgian Code on Corporate Governance (Lippens, 2004), and the codes of good governance worldwide as captured by Aguilera and Cuervo-Cazurra (2004).

Great economic and social damages resulted from the global financial crisis of 2007-2009 and has brought risk management to the forefront of Corporate Governance requirements; the global financial crisis being another failure enabled by poor risk management at companies and particularly at government regulator level (McShane, Nair, & Rustambekov, 2011). Regrettably research (Borgelt & Falk, 2007; Beasley, Branson, & Hancock, 2009) has shown that although in many instances management recognises risk management as an exceptional tool to assist in managing critical risks in the organisation, they also state that it is also sometimes purported as something that must be done simply to demonstrate compliance with the relevant legislation, and it is not always viewed as a necessity.

As indicated by Lyon and Hollcroft (2012) the explosion of the Deep-water Horizon oil rig by BP in the Gulf of Mexico during 2010, wherein 11 people were killed, is another example of companies not having risk management in line with their own business's internal and external operational risks. Apart from the economic and social damage inflicted on residents as a result of the explosion, wildlife and plants along the Gulf Coast of Mexico were severely impacted. The clean-up cost has exceeded $14 billion (Fowler, 2012), excluding the legal ramifications which could cost BP a projected $40-60 billion (Reed & Werdigier, 2012). "Among the many lessons to be learned from this, one is immediately clear: The debacle represents a failure in risk management, rather than a failure of risk management" (Shimpi, 2010).

Risk management is an expanding field, growing beyond the reach of work done in finance and insurance (Wu & Olson, 2009). Based on research conducted by Arena, Arnaboldi and Azzone (2011), Hoyt and Liebenberg (2011), Adams, Lin, and Zou (2011), and McShane et al. (2011), studies within the insurance and derivatives area have been conducted, and they propose more research be conducted on managing risk in non-insurance and non-financial industries, including in the public sector. They are of the view that due to financial institutions being in the business of pricing risks, they should be a step ahead in this field, but all other industries, mainly non-financial, needs to be able to conduct risk management efficiently and adequately. The processes, procedures and policies addressing organisational risks must be cohesive and be constantly analysed for both the internal and external environment for all organisations (Grant, 2007; McGee, 2005).

This research is meant to give more insight into how the regulatory institutions in South Africa, as well as all types of organisations within the public sector can adopt the

principles of the recently published risk management frameworks as per The King Code of Corporate Governance for South Africa 2009 (King, 2009), Committee of Sponsoring Organizations of the Treadway Commission based in the United States (2009) (COSO is a voluntary private-sector organisation comprising of organisations dedicated to guiding executive management and governance participants towards the establishment of more effective, efficient, and ethical business operations on a global basis, based in the United States. It sponsors and disseminates frameworks and guidance based on in-depth research, analysis, and best practices), International Standards Organisation (Purdy, 2010) (also called ISO 31000 2009), Public Finance Management Act, Act 1 of 1999 (PFMA) (National Treasury, 2010a), which established a legal framework for risk management in the public sector, and finally a Public Sector Risk Management Framework (National Treasury, 2010b) which was developed to assist government departments to manage their strategic risks. The last 2010 framework was developed by the National Treasury in conjunction with the Public Services Commission with a view of aligning the South African public sector with the best practices in this risk management arena.

There has been a specific methodology and requirements that have been designed in the financial risks domain for Financial Institutions. The aim being to manage their risks in trying to reach their objectives as per Basel III which was developed by the Basel committee of the "G7" countries and adopted by South African Financial Institutions Regulator giving clear guidelines on how exactly risk must be managed. No such methodology has been developed for public sector organisations relating to the guidelines for managing business risk. The concept of Enterprise-wide Risk Management (ERM), being the strategic risk management concept, is "a relatively recent management activity and has not been fully implemented in most organizations especially those in the public sector." (Cooper, 2010, p. 4). ERM is about taking a holistic, company-wide approach to managing a company's risk, and aggregating information centrally in the organisation regarding various different risk exposures" (Alviniussen & Jankensgard, 2009, p 178).

According to Fraser and Simkins (2009, p. 432) there were only "five case studies published or co-authored by academics on ERM and published in academic journals, only case studies published in journals not books were examined". Therefore it is critical that more case studies in this field are conducted. Internationally a lot more work has been done to guide governments at all levels on how to implement the risk management frameworks, mainly in the United Kingdom, but there is still no clear

consistent methodology that can be implemented by the regulatory bodies within the public sector to apply the stated frameworks (Chapman, 2006; Treasury, 2004; National Audit Office, 2011).

Public sector risk management does not always match the current guidelines from the frameworks (Hood, Asenova, Bailey & Manochin, 2007) as it goes far beyond financial risks to the diverse internal and external needs of societal uncertainties related to service delivery and the public servants employed by these organisations. This research intends to contribute to this field of study by conducting a case study in a public sector institution. These are more qualitative and more soft risks as they are not quantitative but they still need to be managed in the public sector like the normal business risks (National Audit Office, 2011).

Appropriate risk assessment and management may significantly contribute to success in strategy and planning as well as overall operations of the public sector organisations, and is an area that needs further research, including understanding how risk management varies across different public sector activities (Cooper, 2010, p. 5) to strengthen risk management in the public sector. It was found that risk decisions and organisational cultures are complex processes and systems, the need for a common methodology and approach to address risk management at all levels of the public sector is noted, therefore clear risk management practices are necessary for the public sector to focus its resources on the key strategic risks (Hood et al., 2007).

1.2 What evidence verifies the identification of the problem

Cooper (2010, p. 9) states that the provision of health care, education, protecting the environment, regulating the industries, payment of social services and many more, are some of the services that different government departments are tasked with. Cooper (2010, p. 9) further explains that all of these objectives come with some degree of risks and generally the resources expected to deal with these strategic, operational and compliance risks are inadequate. Non-profit ventures and government initiatives can fail “simply because of inadequate attention to one or more of the variables to which the enterprise is vulnerable to, there is a clear need for any enterprise to integrate risk management (RM) within the strategic or business planning of the incubation of businesses and government departments, and to embed these risk processes in all activities that are subject to change or that pose a potential threat to the enterprise” (Heyneke, 2010).

Only 7 percent of risk managers in Australia, the Asia Pacific, Middle East and Africa, Europe, North America and Latin America, rate themselves at an “advanced” level in terms of implementing their enterprise risk management programmes, while over one-third are really just getting started in enterprise risk management, according to a survey by AON-Analytics (McDonald, 2010).

According to Chapman (2006, p. 287) although there is no universally accepted definition for economic risk, it is explained as “the influence of national macroeconomics on the performance of an individual business” which affects the businesses in the public sector and ultimately a country and all its citizens, this is also directly influenced by risk management in public sector. “One needs a strong compliance (hard) state (as opposed to the soft state) which in cooperation with, but if necessary without the market, takes care of the socially needed institutions out of the idea that the process of economic development is first and foremost to be seen as a process of expanding the capabilities of people” (Tshishonga & Vries, 2011).

Private and public organisations globally are realising the importance of a focused and streamlined management of the risks which are embedded within operations that are being undertaken by them (Lyon & Hollcroft, 2012). Over and above the specific processes that are being followed in the business operations, most entities have invested substantial amounts of money and other resources in specific operational risk management systems (De Vries & Nemec, 2013).

The King III report of good governance requires organisations to put risk management practices in place mainly to avoid corporate disasters characterised by company names such as Barings Bank, Daiwa Bank, the Mirror Group Newspapers and Enron who were the agents and examples that led to the birth of a “comprehensive” enterprise-wide approach as has been set out recently to crystallise guidelines for a new era of enlightened management through the risk lens. All these names are tied by a common thread of deficiency in the risk management practices coupled with the absence of oversight where governance was weak and losses were hidden in non-existent accounting entries by key individuals in leadership roles entrusted with the responsibilities of high integrity.

Within the public sector, the law enforcement agencies for national governments are also governed by specific legislation which require them to focus their inadequate resources in key areas to yield maximum compliance and minimise compliance risk.

One such legislation is the PFMA (sections 38(1)(a)(i) and 51(1)(a)(i))(National Treasury, 2010a), which require Accounting Officers to ensure that their institutions have and maintain effective, efficient and transparent systems of risk management for the South African environment. Similar laws in the UK (Public Financial Management), Australia (Australian Public Service Act 1999) and in the US (The U.S. Government Performance and Results Act (GPRA) of 2010) have been implemented driving the importance of structured risk management in enforcing the public sectors' laws.

Romzek, LeRoux and Blackmar (2012, p. 442) noted a disconnect between the sense of accountability displayed by public sector officials as opposed to the literature, with the bulk of the public management literature transactions being based on formal accountability, however, inter-organisational forces reflect underlying norms and expectations associated with informal accountability. Therefore there might be some discrepancies and disconnection between the two notions of what the law is stating and the understanding or expectation within organisations where officials in the public sector still lack a sense of accountability and an active risk management culture. This is important because a culture of risk management is a basis of the requirement of setting the risk management architect in an organisation (King, 2009).

1.3 What is the relevance of this topic to business in SA

It is critical that the regulators or law enforcement agencies maximise compliance to the laws to create an environment whereby businesses and the economy can thrive as this will simultaneously lead to prosperous communities as submitted by Lederman, Mengistae and Xu (2013), and Visser (2010). The Global Competitiveness Report requires strong institutions to attract foreign direct investments, and the Global Competitiveness Index framework 2013 reiterates clearly in its pillar one the importance of strong institutions (Schwab, 2012).

According to Clarke (2012) the power and reach of government agencies and corporations have increased greatly in the last few decades. The prospects, and threats, inherent in so-called "public private partnerships" now loom large globally. Reductions in public sector fraud will contribute to the safeguarding of jobs in the public sector, enhancing the quality of public services and delivering value for money to taxpayers (Clarke, 2012). This is especially by the businesses participating in the economy of the country. Fraud in the public sector was estimated at £25 billion in the UK as published by the national fraud authority and it is stated that 60% of discovered

fraud is by mere accident (Jackson, 2013). A scenario like this amplifies fraud risk management at all levels and mainly at the strategic point of the organisations in the public sector. This is relevant to South Africa due to the prevalent rate of fraud as is part of the formation of any emerging society.

1.4 Purpose and Scope of the research

Effective public sector management is a critical ingredient for sustainable development in Africa especially. Consequently, public sector reform remains a necessary and an on-going policy objective for African countries (Hope Sr & others, 2013). This is being done to overhaul its administrative system to better serve the needs of both government and the citizenry with improved delivery of public services to reduce poverty, improve livelihoods and sustain good governance (Hope Sr & others, 2013).

1.4.1 **Purpose of the research**

The purpose of this research is to investigate a specific methodology together with the risk management practices influencing decision making for adoption by the regulators and law enforcement agencies for state governments. This will be in order to maximise the likelihood of available resources as employed by the government yielding maximum impact in the desired areas where non-compliance risk can be detrimental to the businesses operating in this country as well as the civil society at large. This research is aimed at providing answers to the questions:

1. How do public sector organisations or agencies utilised by the government to achieve government's goals determine their business or strategic risks, operational risks as well as compliance risks in a formal structured methodology as prescribed by Public Finance Management Act, King Code of Corporate Governance for South Africa 2009 Report and Public Sector Risk Management?
2. How the risk management system as determined above gets embedded into the most efficient method of delivering service to the public leading to compliance levels increasing and managing external risk?

1.4.2 **Scope of the Research**

This research is limited to Regulators also referred to as the Law Enforcement Agencies of the government of South Africa. The private Regulators within certain industries are not covered by the risk management methodology being researched

herein because only the public sector institutions will be investigated. There are various government agencies enforcing different kinds of laws as set by the policy making division of the government and only these agencies are covered herein.

A risk management methodology has been implemented by a specific public sector institution based on the Risk Management frameworks (ISO 31000, King lll Report, South African Treasury's Public Sector Risk Management Framework and the COSO Risk Framework) and this research seeks to give more insights into the strengths and the weaknesses of this methodology. The aim thereof is making lessons available from a theoretical point of view for other regulatory institutions and any risk manager in the public or private sector to gain an understanding of how the public sector regulators can apply the risk framework principles in an effective manner. The name of the institution has been withheld to safeguard its practices from exposure as requested by the institution concerned.

The research will cover the actual policies, processes, procedures and risk management practices being employed by an institution in the public sector which will be used as a case study in order to strategically and operationally manage both the internal and external risks faced by the organisation.

2 CHAPTER TWO: LITERATURE REVIEW

2.1 Overview of Literature review

The literature review has been divided into four parts: **Risk, Strategic Risk and Operational Risk** definitions and their explanations set the scene in part one of the literature review, by channelling the reader into a specific area of interest within risk. Then risk is contextualised into an organisation-wide system into the **Enterprise Risk Management** framework being the core of the discussion where risk management is discussed in part two of the literature review. It is at this point that the environment being the **Public Sector and Regulatory Institutions** are introduced into the study to give the required background and the context in this research in part three. Also in part three the indications of innovations that currently take place in public sector and a comparison of public sector and private sector is then discussed within the regulatory institutions framework. When the environment is known then the actual **Enforcement with the related compliance** is outlined in part four as a final part of the literature review.

2.2 Risk, Strategic Risk and Operational Risk

2.2.1 **Risk**

The literature on management has long given some understanding of risk, with Keynes (1937) describing risk as a scenario where probabilities are known and uncertainty was described as where probabilities are unknown (Bernstein & Bernstein Peter, 1996; Hopkins & Nightingale, 2006).

Risk can be defined as uncertain future events that could influence both in a negative and a positive manner, the achievement of the company's objectives. It is the combination of the probability of an event and its consequence. Risk is a condition in which the possibility of loss exists. In some situations risk arises from the possibility of deviation from the expected outcome or event. Risk arises as much from failing to capture business opportunities when pursuing strategic and operational objectives as it does from a threat that something bad will happen" (King, 2009, p .56).

Therefore you may look at risk also as an unwanted outcome, actual or potential, to the institution's service delivery and other performance objectives, caused by the presence of risk factor(s). Some risk factor(s) also present upside potential, which management

must be aware of and be prepared to exploit. This definition of “risk” also encompasses such opportunities (National Treasury, 2010b). Put in another way, risk is the effect of uncertainty on objectives (Purdy, 2010).

Cultural theorists such as Nocera (2009) have shown us that risk means different things in different organisations, while experience has taught risk managers that a given risk model will work in some contexts and not in others. The view explained here indicates that there has to be some objectives for anyone to begin thinking about risk. There will never be any management of risk if there are no clear objectives, meaning that risk experts will never operate in a vacuum, it is always within a certain context.

2.2.2 **Strategic Risk**

Chapman (2006, p. 287) explained that there is no universally accepted standard definition of strategic risk. This is due to the complexity of the concept of strategic risk; there is no quantitative measure that can be able to satisfactorily give a strategic risk measure. He further noted that this is evidenced by the theories that show that those risks that can be quantified as closely as possible are the ones that the academic researchers as well as the risk experts give their attention to, while the qualitative risks, or soft risks, despite how significant they have been, get the least attention (Gates, 2006).

When it comes to risk within strategy, Slywotzky, Drzik and others (2005, p. 80) have defined strategic risk as “an array of external events and trends that can devastate (an organization's growth trajectory and shareholder value”. Chapman (2006, p. 225) goes further defining strategic risk as: Adopting the wrong strategy, failing to execute a well-thought out strategy or not modifying a successful strategy over time to reflect changes in the business environment are forms of operational risk. Chapman suggests then that, strategic risk may be defined as the risk associated with the initial strategy selection, execution, or the modification thereof over time that result in a lack of achievement of overall objectives.

An alternative definition proposed by Johnson, Scholes and Whittington (2008, p. 369) indicates that “strategic risk can be seen as the probability and consequences of a failure of strategy”. A profound feature of Johnson and Scholes’s definition is in the way that focus is placed on ‘strategic’ and not on the ‘risk’ element solely. This may certainly be of paramount importance specifically to the public sector where the

development of the strategic plans is an important part of governance and operations with impact at country-level.

The key focus to the concept of strategic risk is not on the management of the risks but on the strategy itself as it would have been outlined, according to Chapman (2006). The public sector organisations need cohesive plans and strategies that will meet the wider societal objectives and they should be concerned not to implement a strategy that will not work. It is clear from the literature on risk and strategic risk above that the core subject of strategic risk is adopting the correct strategy, executing it in the best possible manner and finally aligning the strategy with the changes in the environment continually.

All three elements have to be in total synchronization to minimise and eliminate strategic risk. This research is concerned with the risks specifically related to formulation, execution, and the on-going interrogation of the implemented strategy with the ultimate aim of having as much compliance as possible by the public sector institutions to their given mandates and from the regulated parties of these institutions.

Strategic management, being a natural step whenever strategic risk has been identified, may be defined as “the appropriate and reasonable integration of strategic planning and implementation across an organization (or other entity) in an on-going way to enhance the fulfilment of its mission, meeting of mandates, continuous learning, and sustained creation of public value” (Bryson & Alston, 2011).

2.2.3 **Operational Risk**

At a non-strategic level of an organisation, an operational level, past the executive layer of the organisation, the risk becomes operational risk. Peccia (2001) states that operational risk is “the potential for loss due to failures of people, processes technology and external dependencies”. Some of the sources of operational risk are outsourcing, reputational risk, systems risk, and regulatory risk relating to lack of observance, certain legal risks, information technology risk, crime risk, and business risk (Chapman, 2006). The method and process of managing risk for the enterprise is explained below.

2.3 Enterprise Risk Management

Von Wangenheim, Silva, Buglione, Scheidt and Prikladnicki (2010) outlined risk management as a systematic process of identifying, analysing and responding to risk. It includes maximising the probability and consequences of positive events and

minimising the probability and consequences of adverse events to objectives. Risk management has six steps. They are risk management planning, risk identification, qualitative risk analysis, quantitative risk analysis, risk response planning, and risk monitoring of controls. The Australian/New Zealand Standard by Knight (2010) sets out its five steps for risk management as (see Figure 1 below) establish the context, identify the risks, analyse the risks, evaluate the risks and treat the risks. Put differently, risk management is the process by which business organisations proactively determine the types and levels of risk appropriate for achieving the organisations strategic goals (Bainbridge, 2009).

The basic process steps are outlined in Figure 1 below:

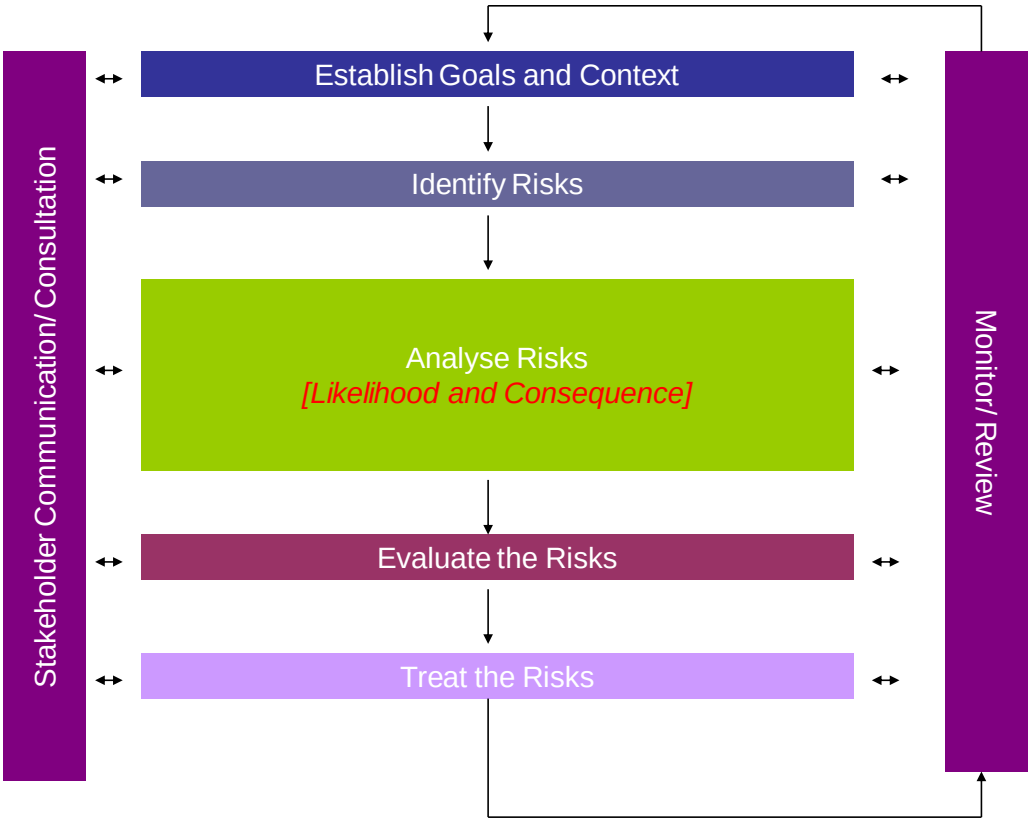


Figure 1: Enterprise Risk Management Process ISO 31000 (2009)

Enterprise Risk Management (ERM) is about taking a holistic, company-wide approach to managing a company's risk, and aggregating information centrally in the organisation regarding various different risk exposures" (Alviniussen & Jankensg\aard, 2009, p 178). The difference between risk management and ERM is in the approach to managing risk, where a corporate approach is followed risks are managed centrally and aggregated in the central point in an organisation, but where risks are managed

independently of each other, “the latter is usually referred to as the “Silo Approach”, whereas the former is referred to as Enterprise Risk Management” (Alviniussen & Jankensg\aard, 2009, p. 187).

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed a COSO-ERM framework in line with the ISO 31000 (see Figure 1), an integrated framework to assist organisations with an encompassing approach and a way of recognising and managing risks. “Enterprise risk management is a process, effected by an entity’s board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives” (COSO, 2004, p.2).

Wu and Olson (2009) submit that their research has discovered that risk management can be used as an instrument for superior rewards and not just as a mechanism against loss. They submit risk management practices and systems have been adopted by many scholars in diverse regions for exhibiting reasonable aspects of dissemination channels, for emerging expertise to support in risk control across supply chain, for managing supply chain risk and for managing enterprise risk.

Even though risk management standards are supportive to embark on a risk management process, they do not benefit to indicate correct tools for risk identification and analysis. In addition, it does not deliver any indication on risk factors/events that might need to be addressed in order to manage risks effectively (Dey, 2012).

Risk management reflects a desire to improve decision making under uncertainty to maximize the benefits and to minimize the costs. Risk management has become increasingly important in modern society as the public shows growing desire for better quality education, safer foods and drugs, cleaner environment, safer products and much higher standards of living altogether (Hill, 2001).

Lyon and Hollcroft (2012) explain the high importance of risk assessment being a combination of risk analysis and risk evaluation per Figure 1 above. This presents the sophistication of the process and clarifies that the risk treatment yields nothing if the assessment is not accurate. Lyon and Hollcroft (2012) bring forward the ten pitfalls that hinder accurate risk assessment as failure to:

- Perform formal assessments as evidenced by the research by Fortune 500 Companies discovering that 65 percent of serious incidents which goes wrong are due to companies' lack of formal risk assessment of their strategies especially the small companies; a checklist alone don't work.
- Define the context & objectives of the assessment
- Understand an organisation's acceptable risk level
- Assemble the best team to perform the risk assessment
- Use the best risk assessment techniques
- Be objective & unemotional in the Risk Assessment process
- Identify hazards that create risks and consider combined whole-system risk
- Consider the hierarchy of controls and failing to prioritise based on risk
- Perform risk assessment during the design/redesign phase
- Communicate before, during and after the risk assessment.

Risk management is the identification and evaluation of actual and potential risk areas as they pertain to the company as a total entity, followed by a process of either avoidance, termination, transfer, tolerance (acceptance), exploitation, or mitigation (treatment) of each risk, or a response that is a combination or integration (King, 2009).

The Comptroller General of the United States (Goverment Accountability Office, 2008) defines risk management as a process that helps policymakers assess risk, strategically allocate finite resources, and take actions under conditions of uncertainty. One major question that still needs to be tackled within ERM implementation is whether the risk events that are rare to the organisation, but should it happen the implications would be massive, should have resources dedicated to them or not? Or, should the bulk of the resources be dedicated to risk events that are more common but carry less liability (such as minor vehicle accidents)? The answer falls back to the organisations responsibilities and priorities as resources are always scarce and have to be intelligently allocated (Kallman & Maric, 2004).

According to Mikes and Kaplan (2013) due to the "many disasters" and corporate scandals that happened including Lehmann Brothers, WorldCom and the September 11 event in the USA, where the actual operational risks were not monitored, the risk frameworks have been designed with the intention of guiding organisations on how to look at all risks and use the framework to have sight of the risks facing the entire organisation from all possible angles. The common thread that was discovered was framed towards risk management becoming a corporate governance requirement

giving rise to the ERM frameworks as we have them now with the country credit rating agencies like Moody's and Standard & Poor's (S&P) also focusing on energy, financial service and insurances sectors and calling for them to implement ERM in order to increase their country credit ratings (Desender & Lafuente, 2012).

Public sector organisations are not focused mainly on profit, but have the accountabilities to use their resources sensibly, governmental agencies are responsible for their risky behaviour (Ross & Bodapati, 2006). The influence of deprived risk management practices with reference to not for-profit or charitable organisations is an added challenge to quantify. If an organisation of this type is inhibited in its ability to render services to its clients or if poor management of its organisational risks takes assets away from the intended purpose, the harm of poor risk management practices is felt, it should be pointed out that risk is not just the actions of one's self but sometimes stems from the actions of another (Hutto, 2009). Good risk management practices should be proactive, not reactive (Hutto, 2009). The recognition of a risk environment is critical, followed by steps to correct or eliminate it (Slahor, 2006).

ERM provides a general view from which any harm that can happen to the organisation can be observed (Wiklund & Rabkin, 2009, p. 55). Mikes & Kaplan (2013) have an opposing opinion; they view these frameworks as the downside of risk management. The fact that risk management is still emerging and has not reached a maturity stage is based on a ten year field study and over 250 interviews done by Mikes and Kaplan (2013) and Coetzee and Lubbe (2013). They therefore suggest that ERM frameworks, principles, guidelines and standards are just not giving the results that are needed. "These reference frameworks do not give the required specifications of which type of risks exactly needs to be managed". They therefore suggest that until we can give a complete framework, we should do away with frameworks.

Mikes and Kaplan (2013) submit that the theories are inadequate and insufficient because Standards and guidelines that aspire to be "applicable to all organizations" and "all types of risk" themselves run the risk of being so general that they lack specific meaning. It is argued by them that prematurely standardising these concepts and principles of risk management is sacrificing the capacity for innovation which is crucial to an emerging and an open-to-all field such as risk management.

Bonisch (2012) noted that in the face of the fact that many analysts find this position of standard ERM frameworks unsatisfying at this stage of the risk management venture,

we can absorb and add by studying risk practices, therefore the different risk management practices needs to be studied further. The frameworks as given currently depend on context and may not always work as they can't help to identify what is risk, how to assess it and the action to be taken to mitigate the risk may not be valid. It is due to this lack of clarity that this research is conducted in the public sector area to gather more insight.

The small number of field-based studies of ERM indicate towards a diversity of practices across organisations, in the same industry (Mikes, 2009; 2011) and even within the same organisation (Hall, Mikes, & Millo, 2012; Woods, 2009). Arena, Arnaboldi and Azzone (2010) undertaking three comparative case studies to detect a constant and developing a collaboration between pre-established management practices and ERM, makes the latter unique to each organisational setting. Due to the complexity of the different risks faced by any enterprise, organisations have put in place different processes and structures in the hope to mitigate and manage those risks (Mikes & Kaplan, 2013).

Notwithstanding this greater focus on ERM, many organisations seem to be disgruntled with the way risk management practices are implemented (CFO Research Services and Towers Perrin, 2008; M. S. Beasley, Branson, & Hancock, 2010).

2.3.1 **Reasons for ERM adoption**

A number of studies seek to link various firm–specific and unambiguous characteristics with ERM adoption. Therefore the reasons for most organisations to adopt ERM have been studied and reasons include leverage, leverage has been found to be a significant determinant as direct economic benefits were clear as opposed to prior to ERM adoption (Pagach & Warr, 2011). Numerous studies agree that size has a significant effect on ERM (Pagach & Warr, 2011). Therefore the big corporates and institutions would be more likely to adopt than small firms.

CEO incentives also seem to impact the way organisations implement risk controls, which tend to be more imperative when management could more likely take greater risks (Pagach & Warr, 2011; Ellul & Yerramilli, 2013).

The normative literature on the subject reflects (Committee of Sponsoring Organizations of the Treadway Commission, 2009; Purdy, 2010), that many scholars contend that ERM adoption is more likely in firms evidencing effective corporate

governance (Ellul & Yerramilli, 2013) therefore corporate governance may be another reason.

The other element is the presence of the risk specialist in the organisation (Desender & Lafuente, 2011; Paape & Speklè, 2012). This individual will more likely ensure that ERM is implemented.

Other theorised ERM determinants, such as institutional ownership and auditor influence, have indicated mixed results (Pagach and Warr, 2011; Paape and Speklé, 2012; Desender and Lafuente, 2011). The influence of auditors can be a reason for ERM adoption.

Regarding regulatory pressure, as the most obvious candidate to explain ERM implementations, the results reported that Canadian companies cited compliance with Toronto Stock Exchange (TSE) guidelines as the third most important reason (37%) for their ERM adoption. Stock exchange listing was a determinant for ERM implementation failing which companies could not continue to be listed with no ERM implementation as per Paape and Speklé (2012).

2.3.2 **Benefits of ERM: Why is ERM important?**

Some risk management guidance advocates that ERM is not only about reducing the impact of negative events, but also about the identification of opportunities (Purdy, 2010). Moreover, by adopting an ERM approach to risk management, firms should be able to improve the way they allocate their resources, this should lead to better capital efficiency and greater return on equity (Hoyt & Liebenberg, 2011). In addition, ERM might induce better risk management disclosures, reducing by the same token the costs of external capital and regulatory scrutiny (Hoyt and Liebenberg, 2011).

While in some firms risk management assumes the role of policing the business for compliance with risk limits and risk policies, in others it may also include processes that help the organization learn about uncertainties in order to turn them into “manageable risks” (Mikes, 2009; Hall et al., 2012).

It has been noted by the Small Enterprise Development Agency in South Africa that an estimated 70 to 80 percent of SMME’s in South Africa failed because they did not have any formal risk mitigation system from the onset of the business (Heyneke, 2010, p.2). This lack of mitigation controls could be a result of a lack of understanding of the enterprise risk management (ERM) methodology or an inappropriate ERM decision–

making model to assist them in a way that would mitigate their risk and minimise financial losses. The ERM approach can anticipate unplanned occurrences and is a systematic way of foreseeing the future (Heyneke, 2010, p. 2).

Organisations have to tailor the risks they are faced with in line with their own units, processes and structures in a way that suits them best (Power, 2012). Kaplan and Mikes (2012) argue that the important point with risk management systems is in assisting organisations in choosing the strategies that will yield the highest returns on investments. This will assist organisations to have a systematised view of the risks that the strategy will come with, therefore channelling the decision makers to actively interrogate the risks and be in a position to minimise the risk as much as possible is vital. This will be achieved through coming up with cost effective ways of mitigating the risks at the same time putting the organisation at the high end of the competitive advantage slide. In this way, the risk management process would influence the companies and institutions to always modify their strategies and position themselves at a lowest risk and highest rewards profile regarding their strategy.

Some risks require a new risk culture altogether as they are new developing risks, some are business as usual. The crucial element is to avoid attaching blame to any risks and instead incentivise the risk disclosure in order to have resources in place responsible for minimising all possible risks. The allocation of resources based on risk is also driven from this point (Kaplan & Mikes, 2012).

Kaplan and Mikes (2012) linked their risk management processes to their strategy mapping processes more than to the resource allocation process, whereas, Woods (2009) linked risk management process to performance management in the balanced scorecards. Mikes (2009) also realised this and came up with what he named risk-based performance management as a way of linking risk management into the organisation's existing processes and procedures.

2.4 Public Sector Regulatory Styles

Regulatory Institutions in public sector are government agencies that formulate and implement regulatory policies; regulatory enforcement behaviour has been compared to the outcome it brings out especially in the developing countries (McAllister, 2010). A common factor about the enforcement of laws in developing countries is that the written laws are mainly sufficient, the obstacles becomes the weakness in the implementation and the enforcement by governmental agencies (Lo & Fryxell, 2005).

Agencies in charge of regulating the law have a propensity to not possess the power to deal with the regulated entities and they seem to have political interests (Drummond & BARROS-PLATIAU, 2006). These regulatory agencies are mostly not adequately funded, leading to low salaries for the employees and ultimately a thriving and constant corruption (Van Rooij, 2006).

These weaknesses in the system relating to the Regulatory Institutions are hampering the implementation and achievement of the objectives and are paralysing even the best policies designed (Skocpol, 1985). Regulatory institutions need to have the ability to formulate and also pursue their goals with maximum autonomy (Skocpol, 1985).

Regulatory agencies that vary significantly in terms of their autonomy and capacity as well as their degrees of formalism and coercion can be characterized and compared along the spectrum as stated in the Table 1 below (Schwartz, 2003).

There are two ways that enforcement of the policies can be implemented by the government agencies. Enforcement style describes how regulators interact with regulated entities as they seek to gain compliance with the law. Research on enforcement style involves "an inquiry into the day to day interaction between the regulatory official and regulated enterprise". The first is the legalistic style which is more concerned with the coercion and compulsion and is primarily about applying punishment for the breaking of the rules (Hawkins, 1991). The second enforcement style is the conciliatory style that is more rooted in techniques of education, advice, negotiation and persuasion (Hawkins, 1984). A study of these enforcement styles relating to the outcome based on how effective the styles are was done (Harrison, 1995) and four dimensions were discovered per Table One below.

Dimension	**Description**	**Spectrum of Ideal Types**
Degree of Formalism	How flexibly agencies apply rules	Flexible, particularistic → rule-bound, rigid
Degree of Coercion	How agencies react to identified violations	Educational, persuasive → threatening, punitive
Degree of Autonomy	How agencies formulate and pursue enforcement goals	Externally influenced → insulated, mission-centered
Degree of Capacity	How active agencies are in identifying violations	Restrained, reactive → energetic, proactive

Table 1: Dimensions of Enforcement Style: (McAllister, 2010)

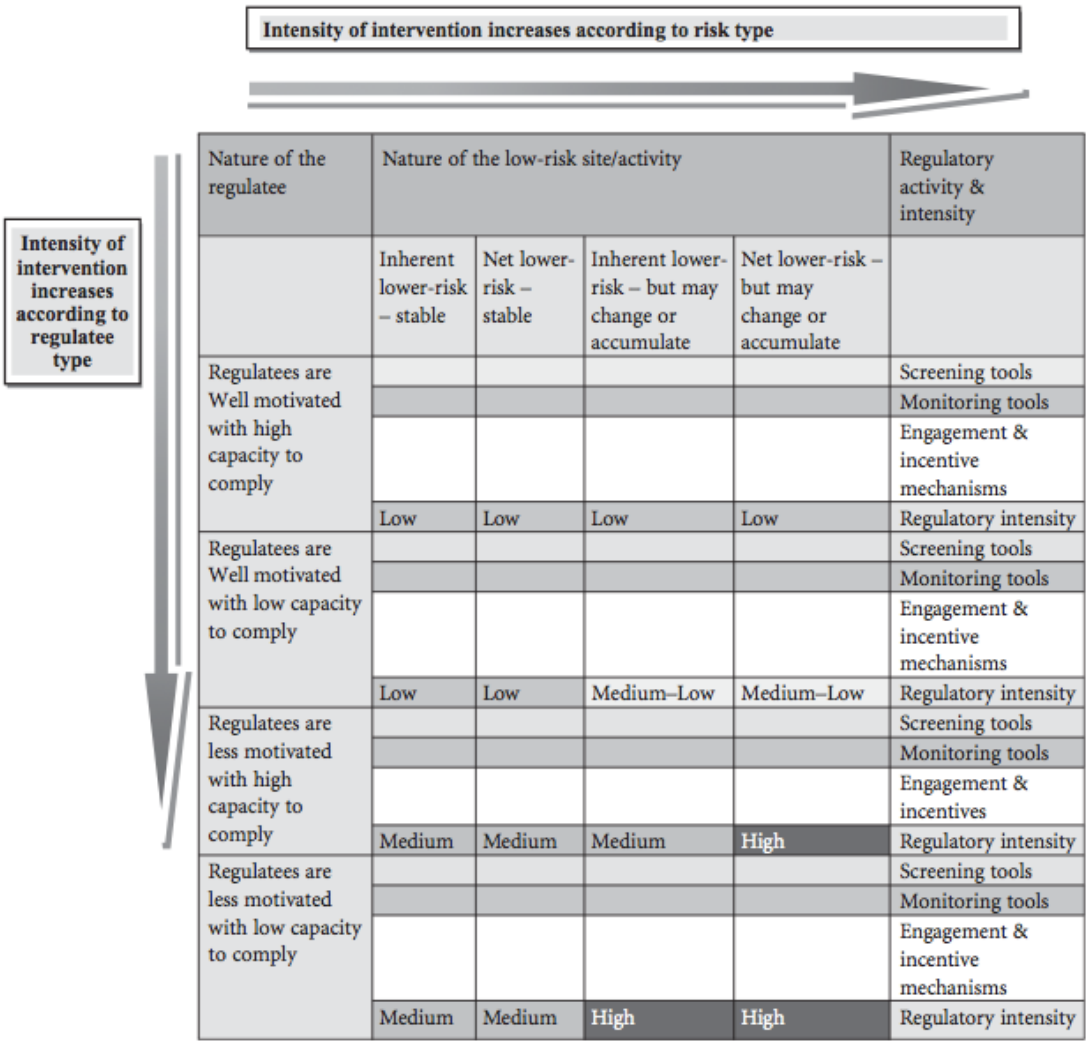
Kagan & Scholz (1980) discovered that whether regulatory institutions are dynamic or inactive "unfortunately has received little scholarly consideration". Braithwaite, Walker and Grabosky (1987) consider "proactiveness" as a characteristic that could not be related to the traditional spectrum of enforcement styles. Studies that paid attention to the capacity and effort level of regulatory agencies consider the effort taking nature of agencies not a type of enforcement style. May and Winter (2000) consider effort an enforcement action rather than an aspect of enforcement style. Black and Baldwin (2012) produced an alternative framework taking the "middle ground" between risk analysis and formal enforcement action. The Good Regulatory Intervention Design (GRID) (see Table 2 below), which provides a framework to categorise sites or activities on the basis of two factors being, the nature of the risk and the nature of the regulatee.

Regulators are then required to adopt only a single strategy, but, this may be unreasonably constraining, and, in some instances, may lead to ineffectiveness (Simon, 2010). In the United Kingdom, Her Majesty's Revenue and Customs (HMRC) institution as well as the Australian Tax Office, for example, categorises all their regulated parties based on the propensity to abide by the laws as anticipated by the authorities (Black & Baldwin, 2012). Based on this the authority then allocates its resources accordingly. This type of targeting by the regulators can assist by deciding the appropriate intervention to be applied to the type of regulatee. This poses a disconnect between the risk based targeting and allocation of resources to the relevant sites and activities and the behaviour based method of allocating limited resources to sites and activities concerned (Black & Baldwin, 2012).

A general strategic framework was created by Baldwin and Black (2008) and Black and Baldwin (2010) to breach the gap between risk and behaviour now updated (Black & Baldwin 2012) as per table below.

Strategies for regulating low risks:

Table 2 GRID matrix



Intensity of intervention increases according to risk type

Intensity of intervention increases according to regulatee type

Nature of the regulatee	Nature of the low-risk site/activity				Regulatory activity & intensity
	Inherent lower-risk – stable	Net lower-risk – stable	Inherent lower-risk – but may change or accumulate	Net lower-risk – but may change or accumulate	
Regulatees are Well motivated with high capacity to comply					Screening tools
					Monitoring tools
					Engagement & incentive mechanisms
	Low	Low	Low	Low	Regulatory intensity
Regulatees are Well motivated with low capacity to comply					Screening tools
					Monitoring tools
					Engagement & incentive mechanisms
	Low	Low	Medium–Low	Medium–Low	Regulatory intensity
Regulatees are less motivated with high capacity to comply					Screening tools
					Monitoring tools
					Engagement & incentives
	Medium	Medium	Medium	High	Regulatory intensity
Regulatees are less motivated with low capacity to comply					Screening tools
					Monitoring tools
					Engagement & incentive mechanisms
	Medium	Medium	High	High	Regulatory intensity

Table 2: GRID matrix: Black and Baldwin (2012)

The other important aspect within public sector regulators as concluded by Yang and Maxwell (2011) is information sharing crossways within organisations. This is a calculated strategic action for organisations in the public and private sector. By means of having a flawless and broad understanding of the dynamics that support and oblige the development of operative systems, support of information exchange and scrutiny, improvement to accuracy and timeliness of decisions, policy makers, and practitioners can advance with superior self-assurance in their outcomes. In addition, researchers can more accurately and efficiently target their research agendas to focus on the most critical aspects of this complex problem.

In instilling the culture of knowledge sharing in public is a need. The advancement of a culture of information stewardship in contrast to ownership; strong leadership backing

to information sharing efforts; legislative and regulatory mandates; reward systems that promote information sharing both within and across organisations; the establishment of shared goals; and the development of on-going trusted relationships based on mutual understanding of needs and concerns and shared responsibility are all positive actions suggested by Yang and Maxwell (2011).

2.4.1 **Innovation within Public Sector and the Regulatory Institutions.**

Gualmini (2008); \vSpa\vcek & Malỳ (2010) outlined that New Public Management (NPM) being public sector in its current form, has improved tremendously globally, it is more product- instead of function-oriented, internally it has become merit-based and careers are organised on a professional instead of formal-legal basis, management-objectives have become dominant over legal arrangements, mobility has increased and flexible work contracts are replacing seniority principles, the bureaucratic ethos are disappearing and the emphasis is on the quality of service delivery and e-government. NPM is meant to improve the quality of the public service delivery on behalf of its customers and on the other hand with an emphasis on the need to downsize the public service, this is a school of thought that there is no way out for the public sector but to leave everything to the private sector and effectively privatise all public sector businesses Gualmini (2008); \vSpa\vcek & Malỳ (2010).

De Vries and Nemec (2013) argue against this thinking. They suggest we still need the government but it must be made as effective and efficient as possible. Due to the developing countries all emerging in differring contexts their related public administration systems will reform to suit differing needs (De Vries & Nemec, 2013). The authors explain that to this end, there will be “common features in NPM from country to country, mainly highlighting the rule of law, reliability, openness and transparency; accountability and responsibility; participation and effectiveness, the need to address long term effectiveness; from an emphasis on efficiency to stressing effectiveness; from emphasizing outputs to outcomes; from input (what is put in) to process (how to do it) thinking”.

De Vries and Nemec (2013) go on to explain that this problem was for a long time buried and hardly addressed under the excuse of neo-liberalism, but entering the second decade of the millennium the problems and drawbacks of a free market without a proper institutional control, cannot be denied anymore. The intense decline in GDP, public revenues and stabilization expenditures divulge the crucial difficulties that many

countries face. It is in those conditions that industries, banks but also common people turn to their governments and request resolutions, which cannot be provided for by the market nor by a minimalistic public sector. It is not adequate just to raise taxes. In such a severe condition it becomes apparent that the one-size-fits-all solution of minimizing the influence of government has serious drawbacks and that the ideology behind NPM has reached its limits.

This also was visible in recent research on developments in Central and Eastern Europe, and as Nemec (2010) argued, the variance in the nature of such reforms and their effectiveness might well be a consequence of varying (extreme) territorial administrative fragmentation in the public sector in countries, the variance in the level of established competition in the market sector, the varying quality of the state of law, the existence of an institutionalized administration in the Weberian tradition being the reaffirmation of the role of states (Nemec, 2010) and the varying extent in which the public administration suffers from corruption.

Akgün, Keskin and Byrne (2012) studied the characteristics of organisations, the level and/or type of innovation relating to certain internal characteristics of organisations such as their size. It was clear that innovation is only introduced if it was part of the strategy and the strategic profile needed to firstly be reviewed within the government authority.

The bulk of the determinations were on improving the efficiency and effectiveness of internal government operations, communications with citizens and transactions with individuals and organisations, by making information and services available on the Internet (Feller, Finnegan & Nilsson, 2010). They submit that e-government is the extensively recognized term and used to describe this phenomenon, and institutes the most demonstrative illustration of the significance of innovation in the public sector currently. Innovation permits organisations to respond to internal weaknesses or external pressures and therefore turn into a vital instrument for decision-making agents all over the world.

This concept also applies to the public sector, where innovation is a useful solution, “the only possible one in the authors' opinion”, during periods with strong economic pressures (Salge, 2011). Wu, Ma and Yang (2012) suggested they will call this type a Collaborative innovation because this name better explains the nature of this innovation type. Process innovation affects both management and the organisation and

changes the relationships between organisation members, impacting the rules, roles, processes, structures, ways of communication and exchange between the organisation members, as well as between the environment and the members (Huarng, Mas-Tur, & Yu, 2012). The connections between Collaborative Innovation which happens through partnering with other organisations and Open Innovation which is new ideas that are speedily taken to the market are obvious (Drechsler & Natter, 2012), as they are both concepts showing that the foundations for invention are no longer essentially internal to an organisation, but have spread to numerous areas in the outside environment. Obviously, citizens also play an important role in the transformation of public services and in their delivery, as they are the users of the services (Eggers, Hansen, & Davis, 2012; Feller et al., 2010).

2.4.2 **Public and private sector differences**

The improvement of costs, productivity and quality of public services is at the core of the adoption of the change management best practices. Considerable amount of work has already been conducted in the area of cross functional teams (CFTs). This is the use of different skills from different areas of the organisation working towards a common goal. Within the private sector, moreover the new product development (NPD) teams whose purpose is to develop new products with the input from all different sections to ensure that the concerns of each division are catered for (Nakata & Im, 2010). There are vast differences in views and knowledge in the bureaucracy in public sector which may lead to unwillingness to co-operate within the independent divisions of the institutions (Nakata & Im, 2010). The work done by Nakata and Im (2010) clarifies the requirement for strong social interconnection group identity as a means of encouraging ‘‘de-individualisation’’ and a change towards interdependent as opposed to independent actions.

For CFTs to be effective in the public sector there has to be goal congruity across the different functions. The differences in decision criteria and timelines is impacting negatively on strategies (Parry, Ferrín, Varela González & Song, 2010). One of the ways which has been found to be more appropriate in dealing with this issue is reward and recognition systems if designed and implemented (Parry et al., 2010). Within the private sector, a team’s ability to perform effectively has been found to be positively linked to rewards.

Therefore in maximising effective performance, quality assurance, risk management and audit functions are gaining increasing importance in public sector management. These practices are achieving acknowledgement and being applied more regularly and strictly in a determination to advance the quality of service delivery, accountability and transparency. This has also improved resource allocation (McComb, Kennedy, Green & Compton, 2008), facilitating teams to finish their projects on time and on budget not challenged by suspensions awaiting additional resources. The other important factor was found to be cultural (or functional) sensitivity in cross-functional integration projects (Nakata & Im, 2010); Parry et al. (2010) found that cultures from staff, management and political levels has to be given attention in public sector for more congruency in functions.

The function and role of quality assurance and risk management throughout the organisation at most public sector still needs to be clarified (Piercy, Phillips, & Lewis, 2012). The authors suggest that the biggest problem is that in general, there is little point in collecting data if it will not be analysed and fed back in some way. It may be easier in a public sector to integrate these roles and processes into the management and operations for value to be created out of new functions.

Piercy, Phillips, and Lewis (2012) further specify that it is important to consider the administrative burden and the impact on morale of processes that are perceived to be too burdensome or heavy handed. This reinforces an issue concerning the need to further explore how to decide how far to go with any of the processes – how to apply them and how much data to collect. It is often difficult to measure the value of effective risk management but we most certainly can see the impact of high profile failures. How to effectively strike the balance would be a fruitful area for further examination.

For public sector the more the citizens can trust the public servants, the more these public servants will have the capacity and the willingness to be helpful and perform their duties the best way they can, and the more the citizens' trust will multiply too (Denhardt & Denhardt, 2011). Mutual trust and cooperation would be achieved only if a "service and client approach" is employed to create an environment where voluntarily participation thrives (Alm, 2012). ERM can greatly assist by ensuring that the type of enforcement style or enforcement action as indicated in Table 1 and Table 2 above is directly aligned to the total organisational goals as outlined in Figure 1. The risks that would have been identified as well as related treatment actions following Figure 1

would have to inform the type of innovation (as stated in section **2.4.1)** that is mostly needed by a public sector institution.

2.5 Compliance levels by Regulators to the regulated parties

Any actions that are taken by regulators to ensure compliance can be broadly termed enforcement action (Zubcic & Sims, 2011). It has been evidenced that there is a decrease in corporate violators after an enforcement action has been exercised. But the subsequent rate of violation does not mean there is a cause and effect relationship, it is still possible that the violators had become more smarter and detection is not easy (Zubcic & Sims, 2011).

In instances where there is a large corporate collapse in Australia, the questions always lead to the effectiveness of the regulators and of the enforcement actions. This has resulted in escalating pressure on governments and regulators to be more protective to investors and hold the violators more accountable for misconduct (Zubcic & Sims, 2011).

Enforcement actions by law enforcement agencies or regulators as a form of corporate governance is becoming more practicable. This is due to increased penalties yielding greater compliance levels. Zubcic and Sims (2011) suggests that beyond penalties, enforcement actions relating to corporate governance also remind directors in corporate that they have responsibilities and there is great risks attached to them not fulfilling their responsibilities. Enforcement actions can take a role of educating broad communities and instil consumer confidence (Zubcic & Sims, 2011).

The authors further state that regulators lack the systematic compliance measurement systems to conclusively prove that a decline in subsequent enforcement actions reflect better compliance. An analysis for two industries that were highly regulated concluded that enforcement actions instil a culture of compliance and does change behaviour of the regulated parties (Zubcic & Sims, 2011). This was affirming that where enforcement is strong, there are increased corporate penalties with convicting and imprisoning executives and publicizing the misconduct, then better corporate compliance can be achieved. This would require a risk based approach to monitor compliance with resources at the disposal of the regulators Where regulatory (Bier & Lin, 2013) decisions are based on risk analysis this has the impact of decreasing compliance costs and reducing risk through escalated management flexibility in achieving acceptable levels of compliance. This points out that existing regulations relating to the

environmental safety requires the affected to self-report to the regulatory agencies (Bier & Lin, 2013).

There is no adequate literature on instances where the regulator relies on the regulated parties to measure compliance levels or reduce the risk. Bier and Lin (2013) outlines that stiff penalties can reduce compliance by the regulated where it becomes worthwhile to not disclose noncompliance rather that challenging a large penalty. Unlike increasing the severity of penalties, it may be worthy to reduce costs of compliance wherein the regulated will automatically be more compliant as it does not cost them much to comply. Due to ineffective strategies, regulators become cooperative to the known violators (Bier & Lin, 2013).

2.6 Summary of Literature Review

Nocera (2009) defined risk as a concept that is only derived after an objective has been set. Therefore risk can only exist within a context of the objective. This then means that risk equals different things to different organisations. When it comes to risk within strategy, Slywotzky and Drzik (2005 p.80) have defined strategic risk as “an array of external events and trends that can devastate (an organization's) growth trajectory and shareholder value”. Chapman (2006 p. 225) and Kaplan and Mikes (2012) go further defining strategic risk as: Adopting the wrong strategy, failing to execute a well-thought out strategy or not modifying a successful strategy over time to reflect changes in the business environment are forms of operational risk. Kaplan and Mikes (2012) linked their risk management processes to the strategy mapping processes whereas Woods (2009) linked ERM to maximising performance management.

An alternative definition proposed by Johnson and Scholes (2006 p. 369) indicates that “strategic risk can be seen as the probability and consequences of a failure of strategy”. This is the basis of what the ERM implementation is about. Strategic management being a natural step whenever strategic risk has been identified may be defined as “the appropriate and reasonable integration of strategic planning and implementation across an organization (or other entity) in an on-going way to enhance the fulfilment of its mission, meeting of mandates, continuous learning, and sustained creation of public value” (Bryson, 2011).

A framework in Figure 1, from ISO 31000 standard, indicates ERM is about taking a holistic, company-wide approach to managing company’s risk, and aggregating information centrally in the organisation regarding various different risk exposures

(Alviniussen & Jankensgard, 2009, p 178). The difference with risk management from ERM is in the approach to managing risk, where a corporate approach is followed risks are managed centrally and aggregated in the central point in an organization, but where risks are managed independently of each other, “the latter is usually referred to as the “Silo Approach”, whereas the former is referred to as Enterprise Risk Management” (Alviniussen & Jankensgard, 2009, p.187). The critics of ERM (Dey, 2012) view the framework as inadequate as it does not clarify the correct tool to identify the risks and the assessment of those identified risks. Additionally, the standards do not indicate which type of risk must be addressed for effective management of risks. Mikes and Kaplan (2013) further oppose ERM suggesting that more clarity still needs to be established before frameworks can be published.

Lyon and Hollcroft (2012) clarified the ten pitfalls (section 2.2) that need to be addressed in order to conduct a more accurate assessment of risks. The allocation of resources also benefits from the ERM (Hoyt & Liebenberg, 2011) resulting in returns on assets increasing.

The literature on the context for this research being public sector regulatory institutions indicates challenges (Lo & Fryxell, 2005) in implementation of laws and enforcing the strategies. Table 1 indicates the possible ways of enforcing laws (McAllister, 2010). Black and Baldwin (2012) in Table 2 show their updated model on how to decide on the appropriate action to enforce the laws. The importance of sharing of information is also highlighted in the literature (Yang & Maxwell, 2011).

The new public management NPM) ideology according to Gualmini (2008); \vSpa\vcek & Malỳ (2010) is outlined as the future of public sector organisations. Efficiency and effectiveness will be at the peak through e-government (Feller et al., 2010). Cross functional teams may be a solution for public sector(Nakata & Im, 2010). Bier and Lin (2013) submit that if decisions are based on risk analysis this has the impact of decreasing compliance costs for public sector.

A gap in the literature within public sector in South Africa still exists as there is no literature relating the public sector institutions and their strategy formulation together with their enforcement styles to ERM. This research has been undertaken to get an insight into how the ERM literature is being applied and the challenges faced or successes within the public institutions can be understood.

3 CHAPTER: THREE: RESEARCH PROPOSITIONS

The review of literature shows that the Enterprise Risk Management framework enables the organisation to view its total possible risks that can impact on strategies or strategic objectives. The creation of a system that extracts risks from all levels and sections of the organisation and centrally managing the key risks at a strategic level is vital in ensuring that all strategic risks are always monitored. The research is geared at understanding how the public sector regulators are implementing this risk management framework as they are required by the legislation to put the methodology relating to risk management into practice.

The literature review suggests that regulators will benefit from putting the risk management frameworks into use which will require the public sector institutions to be innovative and maybe learn from the private sector in order to maximise the compliance levels for both the regulator itself to its own rules and the regulated parties to be managed such that the risks of not following the correct laws are minimised for the benefit of all citizens.

Therefore, this case study will specifically investigate within a public sector institution:

- How the exact risk identification system, risk assessment process, and the system of coming up with risk mitigation action plans as well as the implementation and follow up of the specified action plans are undertaken.
- How the limited resource allocation is impacted by the risk management system
- How compliance by the public sector organisation is impacted by the risk management system being employed by the organisation.

The following propositions have been formulated based on the literature review, for testing:

3.1 Proposition 1:

The adoption of ERM by an organisation enables the view of the organisation–wide risk in a systematic method enabling the formulation, the execution and the continued review of strategy in line with the internal and the external environment of the organisation to minimise strategic risk as defined.

The basis of the formulation of a strategy specifically taking into account the risk management process in Table 1 wherein risk is identified, analysed and assessed then

action plans put in place will be investigated. This needs to be performed during strategy formulation, implementation and review to ensure continuous monitoring of organisational risks.

3.2 Proposition 2:

ERM benefits the organisation in the allocation of resources to capture any opportunities based on a risk management system to create the most efficient method of delivering service to the public.

The research will determine whether indeed in public sector institutions ERM assists to direct the limited resources into areas where the need is at a critical stage.

3.3 Proposition 3:

Public sector institutions will influence compliance levels by improvement of its strategic risk management systems which manages compliance risks.

The research will determine whether indeed in a public sector institution ERM assists to ensure that all rules that need to be complied with are indeed complied with by the institution concerned.

4 CHAPTER FOUR: RESEARCH METHODOLOGY

4.1 Rationale for the proposed research

This study was aimed at uncovering “how” and explaining “why” effective management of internal and external business or strategic risks as well as operating risks facing the public sector regulatory institutions is essential. This can be a key instrument to improving the chances of these organisations being able to discharge their services with the best possible strategy in place, and compliance by the regulators and the regulated parties also has to be kept at the highest possible level.

The management of public sector risks in order to influence compliance is an emerging field requiring more in-depth understanding. “In general, case studies are the preferred strategy when “how” or “why” questions are being posed, the researcher has little control over events, and when the focus is a contemporary phenomenon within some real-life context” (Yin, 2003, p. 1). “How” and “why” questions are more explanatory and likely to lead to the use of case studies. This case study will therefore specifically investigate within a public sector institution:

- How the exact risk identification system, risk assessment process, and the system of coming up with risk mitigation action plans as well as the implementation and follow up of the specified action plans are undertaken.
- How the limited resource allocation is impacted by the risk management system.
- How compliance by the public sector organisation is impacted by the risk management system being employed by the organisation.

This was the preferred research strategy as these questions deal with operational links needing to be traced over time, rather than mere frequencies or incidence (Yin, 2003, p 6). Saunders and Lewis (2012) recommend the use of explanatory studies whereby an explanation behind a particular occurrence through the discovery of causal relationships are determined between key variables. The compliance levels were studied based on the risk management method being employed by the regulator. An induction approach was followed for this research. An induction approach refers to as it had moved from specific observations to broader generalisations thereby creating theory as explained by Saunders and Lewis (2012). The intention of this project was ultimately to add to theory by generalising the results of the research from this case study.

“Case studies are generalizable to theoretical propositions and not to populations or universes” (Yin, 2003, 10). In this sense, the case study does not represent a “sample”, and in doing a case study the goal will be to expand and generalise theories”. “You would use the case study method because you deliberately wanted to cover contextual conditions – believing that they might be highly pertinent to your phenomenon of study” (Yin, 2003, p.13).

Currently in South Africa and within the public sector institutions that are governed by specific laws, there are some organisations that have implemented a risk management methodology as required by the current Public Finance Management Act, the 2009 King III report as well as the 2010 Public Sector Risk Management Framework as published by the National Treasury for all public institutions to adhere to. This research sought to add to the academic theory available with regards to the risk management in the public sector based on the current literature review conducted by the researcher and compare that to how a public institution in South Africa has implemented the risk management framework through designing their own methodologies to achieve the requirements of the framework.

The aim herein was to assist in creating more knowledge academically with lessons from the case study to be undertaken and for public organisations to recognise both the strengths and the weaknesses of their current methodologies based on current literature as conducted by the researcher.

It was with this in mind that an explanatory study whereby an explanation behind a particular occurrence through the discovery of causal relationships was determined between key variables. The compliance levels were studied based on the risk management method being employed by the regulator. An induction approach was followed for this research as it moved from specific observations to broader generalisations and theory as explained by Saunders and Lewis (2012).

The qualitative research strategy that was used was the case study strategy. Saunders and Lewis (2012) reiterated this strategy as stated above by Yin (2003) and also stated that it is meant to answer the questions “how?” as well the “why? “. The main intention here was to investigate the particular situation in a real life context which is similar to the researcher’s problem situation including multiple sources of evidence which were interviewing, observations, relevant source documents and any other evidence the

interview environment offered at that time. The case study method was seen as most relevant in providing the required in-depth understanding.

4.2 Population and unit of analysis

Population was defined as “the complete set of group members” by Saunders and Lewis (2012, p. 132). The population for this research was the public sector institutions in South Africa that had adopted and implemented some form of risk management methodology as part of their strategies to ensure that the organisational internal and external risks are systematically approached and managed. The methodology needed to be in a form that could be assessed independently of the other systems in the organisation with the results before and after the implementation. The population of relevance for conducting this case study was the public sector institutions with operations nationally.

Our unit of analysis was a single institution in the public sector whose risk management methodology was used as a case study to dissect and obtain a full dipstick analysis of how exactly the requirements of the risk management framework for public sector as explained in the National Treasury Risk Framework (National Treasury, 2010b), PFMA (National Treasury, 2010a), ISO 3100 (Purdy, 2010) and the King III report (King, 2009) were implemented to best enable the institution to offer the best services to the country and its citizens.

4.3 Size and nature of sample

A purposive sampling method was followed wherein informant selection is highly relevant for this sampling technique as it is a type of non-probability sampling that is most effective when one needs to study a domain with specific individuals who are directly involved. “Purposive sampling may also be used with both qualitative and quantitative research techniques. The inherent bias of the method contributes to its efficiency, and the method stays robust even when tested against random probability sampling. Choosing the purposive sample is fundamental to the quality of data gathered; thus, reliability and competence of the informant must be ensured” (Tongco, 2007). Furthermore a case study research was undertaken as there was a specific deep analysis for a phenomenon that needed to be investigated through the public institution that approved the research to be performed through. The risk management methodology is not yet a matured phenomenon (Coetzee & Lubbe, 2013) therefore the

methodology is applicable at the top levels of management for now. No employees at the lower levels could be interviewed as they were not yet involved directly.

The sample within the institution was limited to the officials who were directly and indirectly involved in the implementation of the methodology. Semi-structured interviews to senior executives and strategy leaders were undertaken for the case study.

A total of 8 Executives were interviewed within a chosen public sector institution. The interviews were conducted at head office group level with members of the Executive Committee including the Chief Executive Officer. The Executive Committee members were also the members of the Risk Committee and one senior official who was involved in the risk management functions directly. This strata as explained, indicates that interviewees were selected based on their positions and experiences to solicit expert information from them (Saunders & Lewis, 2012). The researcher had the knowledge that there was an enterprise risk management methodology that had been employed by the institution. The researcher also had the knowledge that this public institution had been able to meet its stated targets over the years. At that stage the researcher was not in a position to attribute the success of the institution to the enterprise risk management methodology but some relationship if any would be investigated.

4.4 Data Collection

4.4.1 **Pre Test**

A pre-test was conducted to ascertain the flow and the ease with which the questions can be posed to the respondents. A few changes were subsequently made to the questionnaire to cut the long questions into short clear questions. The appropriate manner in which the questions would be posed was agreed. The information to be communicated prior to the questionnaire being commenced with was also clarified during the pre-test.

4.4.2 **Interviews**

For the case study, a combination of semi-structured interviews and documentary analysis was used (Saunders, Saunders, Lewis & Thornhill, 2011). A major strength of case study data collection was the opportunity to use many different sources of evidence. According to Yin (2009), the use of multiple sources of evidence in case studies allow an investigator to address a broader range of historical, attitudinal, and

behavioural issues. The most important advantage presented by using multiple sources of evidence was the development of converging lines of inquiry which is called a process of triangulation.

Four types of triangulation are the triangulation of data sources (data triangulation), among different evaluators (investigator triangulation), of perspective to the same data set (theory triangulation), and of methods (methodological triangulation). When you have really triangulated the data, it means that the events or facts of the case study have been supported by more than a single source of evidence and this improves construct validity. Data triangulation method was employed in the performance of the semi-structured interviews. This was performed through requesting from the organisation all documents that were mentioned in the interviews to allow the researcher to follow the derivation of any evidence, ranging from initial research questions to ultimate case study conclusions. Some of the risk management reports were documents from the external auditors and service providers who were involved; this validated the information from the audio recordings. Observations of the culture of the organisation as related to risk were also noted.

A database of the case study was created. This increased the reliability of the entire case study. Case study notes, case study documents including annual reports from the website and audio recordings were created as data was collected for each face to face interview using open ended questions with each interview going for about an hour. Maintenance of a chain of evidence was critical to the data collection within a case study.

Per Saunders and Lewis (2012), caution should be exercised to guard against the validity and reliability of data due to common interview error. This is the type of error that may happen when the interviewer is not able to write fast enough and capture all the answers in the most appropriate way. This may result in the loss of very important information. The researcher made use of audio recorder with the consent of the interviewee in order to minimise that potential error. A summary of the key notes taken from the interview was reconfirmed with the interviewee just to ensure that the essences of the responses that are critical were captured accurately on the voice recordings.

4.5 Data Analysis

All the raw data that was collected had to be analysed in order to achieve the objectives of gathering information. The semi-structured interviews were all recorded with the consent of the interviewees. The audio recordings were all transcribed to facilitate the process of analysis.

The theme for each question under the proposition as outlined also in Chapter five was used as a code for the analysis. Each respondent's explanation was carefully examined to determine the understanding of the theme of the question and most importantly to check if the respondents did not bring out any unexpected themes from their answers. The researcher was scrutinising each reply per the question asked to all the participants to ensure that the answers indicated appropriate understanding of the concepts and the principles of ERM. A thorough content analysis was performed through extracting and summarising the key point in the responses as given by the participants. All the key details were noted and outlined in the presentation of the results in chapter 5. The analysis indicated which areas were understood and which areas of ERM were not understood by the officials of the institution used as a case study. The table on chapter 5 clarifies the analysis. Only common ideas not frequency of words were used during the analysis.

4.6 Research limitations

The results of this research will be applicable to the regulatory institutions in the public sector only. The sample case study used is in the public sector and due to a case study on one particular organisation in the public sector the results thereof are not necessarily reflective of every single public sector regulatory institution but a generalisation on the issues that are pertinent in the public sector thereby contributing to general theory as intended not serving as a sample to represent a population. A non-probability purposive sampling was used. The study was conducted only in the Gauteng province in South Africa within senior management and executive level.

There was limited time during working hours for the participants. Approximately one hour was taken per interview and some interviews had to be limited to the time of one hour.

The sample was limited to one public institution as the approvals for other interviews within public institutions could not be finalised within the required period that the researcher had requested.

5 CHAPTER FIVE: RESEARCH FINDINGS

The previous chapter, section 4.5 on Data Analysis, outlined the methodology applied to test the research propositions as presented in Chapter Three. This chapter will present the results of the interviews as conducted with the eight senior officials at a public sector institution which has been used as a case study. The understanding of risk management in a public sector organisation has been gathered at a deep level in a qualitative and exploratory method.

5.1 Description of sample and respondents

The sample selection was based on a public sector institution that has implemented a risk management methodology. The specific individuals who were targeted within this institution are senior and executive managers who are responsible for the development and execution of the organisational strategy as well as the strategic and operational risk management system.

Eight requests were forwarded for interviews and eight officials ultimately participated in the interviews giving a 100% positive response rate. Open ended questions, annual reports, internally generated documents, external regulator and policy reports, as well as media briefings were collated in order to form the basis of the findings as collated herein. The results stated herein were compared to the constructs identified in the literature review and were found to be satisfactory. No unexpected themes came out of the interviews that were not covered in the literature.

5.2 Themes of the research questions presented

The subject matter of each of the research questions posed was designed in the questionnaire to get the respondents to reply to specific questions which would ultimately give a clear idea to the research propositions as follows:

1. The basis of the risk management methodology within the organisation, i.e. the risk identification, assessment and mitigation plans against the identified risks;
2. The system of integrating identified risks into the formulation of the organisational strategic objectives as well as operational plans;
3. The significance of the “risk concept” during the formulation of strategy;
4. Risk appetite or the risk tolerance level of the organisation;

5. The comfort levels as far as strategic risk is concerned, is it possible to get to a level where it can be said that all known possible risks have been covered before the strategy is finalised;
6. During execution of the strategy, when the risk profile changes what happens;
7. When and how exactly does the review of the strategy happen in a public sector institution;
8. The significance of the "risk concept" during the review of strategy and the evidence thereof;
9. Risk management as part of the performance indicators;
10. The influence of risk management on the allocation of resources;
11. The influence of risk management on the compliance levels of the organisation to laws and regulations by its regulators as well as the regulated parties which the institution needs to regulate.

5.3 The layout of findings

As the open ended questions that have been conducted were based on a questionnaire that had been specifically designed for the interviews, the layout of the findings will be in line with the theme of each question as was posed whereby the question is proof of the existence or non-existence of the propositions as outlined in Chapter Three.

5.4 Research Proposition 1:

The adoption of ERM by an organisation enables the view of the organisation–wide risk in a systematic method enabling the formulation, the execution and the continued review of strategy in line with the internal and the external environment of the organisation to minimise strategic risk as defined.

To test this proposition, the first ten specific questions relate to risk management within strategy in terms of formulation, execution and strategy review. All eight participants were asked to explain how this is done in their public institution through responding to each of the ten questions relating to proposition one. The actual questionnaire and transcripts of these recorded interviews are all attached as per appendix A and B. Table Three below demonstrate a summary of the respondents.

×= denotes no immediate understanding of the concept

√= demonstrates the understanding of the concept and in line with the other respondents

Respondents:

Table 3 : A B C D E F G H

Proposition1									
Basis of Risk Identification	×	√	√	×	√	√	×	√	5/8=63%
Basis of Risk Assessment	×	√	√	√	√	√	√	√	7/8=88%
Basis of Risk Mitigation Plan	√	√	√	√	√	√	√	√	8/8=100%
Risk consideration in formulation of Strategy	√	√	√	√	√	√	√	√	8/8=100%
Significance of Risk Concept in Strategy Implementation and Review	√	√	√	√	√	√	√	√	8/8=100%
Risk Appetite	×	√	√	×	×	√	×	×	3/8=38%
Proposition2									
Risk consideration in allocation of resources	√	√	√	√	√	√	√	√	8/8=100%
Proposition3									
Risk Influence on compliance levels	√	√	√	√	√	√	√	√	8/8=100%

What forms the basis of risk identification, assessment as well as mitigation plans to reduce the identified strategic and operational risks in the organisation?

As described by the Public Sector Risk Management Framework 2010, ISO 31000, COSO 2009, Chapman (2006), and Alvinniussen & Jankensgard, (2009, p. 178), the Risk Management system that is adopted at an enterprise-wide level enables the organisation to formulate, execute and continually review its strategy and strategic

objectives with a specific view of the risks both internal and external to the institution in a systematic enterprise-wide view including all operational risks.

The operations senior manager explained that previous performance is usually looked at, critical things that may affect the strategy are reviewed and all this information is systematically registered in a formal risk register which is currently implemented and maintained. The goals are then aligned with the related risks. She explained that there is a risk management policy, the strategy document and the annual performance plans that are all considered based on required resources. The assessment of the identified risks as recorded in the risk register is performed with the help of the external service provider. In these sessions the risks will be rated as high, medium or low then it is clear to all divisional managers which risks are critical at an enterprise level this is based on a matrix as provided by the external risk management service provider. The mitigation plans are also agreed upon and then taken through to operational level.

The human capital Executive, further to the above, explained that there is a risk committee that ensures that all risks are managed when the committee meets quarterly. Two risk documents being used, one at a strategic level and the other at an operational level complement each other. They are used to manage risk at each level. He explained that in assessing those risks the management look first at what are the mitigating initiatives that they have, to mitigate the risk or even eliminate the risk, and then look at the prevalence of that particular risk and also extend to the frequency and the likelihood of that risk happening, without those controls put in place. And based on that an assessment, on a year to year basis at a strategic level, as managed by external auditors the risk register is kept. The auditors are the ones that actually give guidance in terms of the risk management principles, to say that the assessment done is an objective assessment and is more or less mirroring exactly relative to the organisation at that moment.

The other respondent explained that after they have developed a strategy as Executive Committee (EXCO) they then have a separate seating whereby they make use of a service provider so they can channel the process as explained above. At that stage the divisional executive would have already consulted with all his senior managers to ensure that all the important risks are understood by him so he can escalate them accordingly. The operational risks from operations help to influence the strategic risks affecting the entire strategy. The operational risk documents are much bigger documents as compared to strategic risk documents as not all risks needs to go up to

strategic level. The related action plans will also be populated into the same document by EXCO and will be accepted by operations before finalisation.

The other respondent explained as follows “we capture them at strategic level as well as operational level, and also on our basic plan. So on the strategic level it is a very high level, but on the operations that is where you will break down in detail, that on the basic contingency plan, that is where we have all the risks in detail”.

The company secretary related the basis of risk management to the mandate that has been given to the institution by the government. She explained that the business and operational risks needs to be actively managed through a clear system to ensure that they are kept at a minimal if not completely avoided. She referred to the political, economical as some of the risks to the achievement of business objectives.

The Chief Executive Officer (CEO) said

“What we usually do only as the basis, we are a state-owned entity, we are governed by PFMA, and also in terms of the requirements we also as we submit our strategic plans, we also need to submit our risk management plan to the shareholder. So that is legislated, but it is also important for us as an organization to understand what are the key risks that happen, that we need to manage”. She went on to explain that the identification process is firstly addressed with the Board of Directors (the Board) to say what are the key risks that really keep them awake at night. And then working together with the internal auditors, a risk register is created wherein the top 20 risks affecting the strategic objectives are identified, then the assessment of each risk, looking at the implemented controls, and action plans. Seeing that this is an essential service organisation something that is greatly critical is the business continuity plans should anything drastically wrong happen. This risk has also been covered through the risk management system. On a yearly basis when the strategy is reviewed the risk register is also reviewed at the Board level through the risk committee and the Board gets an opportunity to give input if there may be some risks that are not covered in the register.

How are the organisational risks integrated and encompassed into the formulation of the strategy or strategic objectives as well as operational plans for the organisation?

A respondent explained that “you have the strategic objectives and then the risks that are talking to them and you do the risk metrics to say is it high level or whatever, and I need this to mitigate that, is it going to be within the budget that we have, or are there some additional resources required to mitigate”.

The other response was that “the strategic plan of the organisation is a point where the organisation wants to be, and factors that ought to be taken into account in working out that plan are the particular strategic risks that have been identified in the organisation that can hinder the achievement of the targets in that, and how we do that, we then phrase or work out an objective that will be directly responding to that strategic risk identified”. He said they also have a strategic risk profile of the organisation, that risk profile gives you the kind of risk profile of the organisation and when you review the strategy you already have an understanding of what the risk profile is and hence when you review your strategy in terms of the attainment of those objectives you will then work out activities or targets that will speak to these risks or alternatively you manage your risks such that they contribute to the objective of attainment of what is in this strategy.

The other respondents summarised by saying: “So we do take into account the risk when we do the objectives, because if I look at all the objectives, they are also linked more to the risks”.

The CEO explained that “When we do the risk identification for our risk register, we identify the risk and then from there we say in terms of the strategy in the strategic objectives that have been set up, these risks, which of these key objectives that it will have the most impact, and then we link the risk to those key objectives or goal. When it comes to operational plan, we allocate different divisions to different specific risk and then they take those identified actions that needs to be taken to start and come up with an operational plan in terms of managing that risk”.

The ICT official explained “that in fact risk management in my view, is part of all of the planning process, whether you are doing strategic planning, in the end everything has to talk to each other”.

The risk official also referred to the PESTEL framework of looking at the strategy and covering all angles.

How significant is the role of “risk concept” when strategy is being formulated?

An interviewee explained that “I think it is important really to understand what is it that the organization wants to achieve in terms of the strategy, but you cannot set the strategy without also really looking at the risks, because the critical thing is as much as you want to achieve and you set yourself goals, the first thing is the strategy must talk to resources. Now the first thing you should ask yourself is do you already have these resources? If we are to change, how well are we going to be able to change? Because that change in itself is a risk in terms of managing that change”.

The other officer explained that the risk profile provides you with signals that you will always have to be aligned to, in the formulation of a strategy as well as the execution of the strategy, because formulation could be a bit easy without a strategy but the test lies in the execution of the strategy and if you don’t factor in the risk profile of the organisation the hindrances will be encountered when you are executing the strategy.

The other response was that “mainly when formulating strategy, operational strategy, we don’t look at the risk in detail. There is another session when we review the risk, which is completely separate”.

The company secretary explained that, if you go to any copy of the strategy documents, there won’t be a single one that hasn’t captured the risk, because even the timing of how they go about doing that, they do the enterprise risk management review in the first quarter of the financial year and the strategy in the second quarter or by the time we go to the strategy we have already identified the strategic risk, so there is no way you can leave those out at all.

The CEO emphasized that “the board takes it very seriously, four or five years ago we didn’t really have a risk committee in place, so we realized it is something that is very important for an organization, so we have put the risk committee; all the EXCO members are members of the risk committee and the CEO is the chairperson of the risk committee and then in each division they also need to have their own champions, however with the board as well, the auditing and risk committee has taken issues of risk very important, and in fact for King III as well, we need to be looking at this. So what we do, after we have submitted the risk register and our internal auditors when they do their three year internal audit plan, they are doing a risk base, so they cannot

do the three year audit plan without working around the identified risk. So that is how significant it is. And as I have indicated, we also need to submit to the shareholder as well".

Does the organisation know how much risk it is willing to take, i.e. Risk Appetite and Risk Tolerance? What is this based on?

A respondent explained as follows, "We have a dual mandate, which is the public good and commercial. So our willingness to take on board the mandate we have, says we have a very good understanding of what it is. So in terms of our planning and everything we have a fair understanding of the risk that we have, to be able to meet this mandate – with very little resources sometimes, because with the public good we have to deliver on that, and we also have to go commercial. But the way we are as an agency, we also get additional mandate, sometimes even without funding. So we are willing to take on board those kinds of deliveries. So to me it tells me we have a very good in-depth understanding of the risk we are taking as an organization. We sometimes don't even know how we are going to find it, but we are prepared to swing in and to say what is it that we can do to improve because it is really about continuous improvement and the fact that we are continuously wanting to improve, to really better ourselves and to deliver according to the mandate of the organisation, we are always looking at what are the national developmental plans, what are they talking about, what are the certain things that we have not ventured into, how do we go about venturing into that to deliver and to remain relevant. And I always say it is the organisation that understands that there are risks that they have to take but at the end, what is it that you have achieved with that? Now we have taken on risks, global client framework, which we are dealing with, which doesn't necessarily have the funding and it is something we are prepared to take on board and say we want to represent the state on these kind of things and we are now putting together the plans to say 'this is what we will do and this is how much it will need in terms of resources".

The other view was that there are those that you would actually take the risk and there are those that we will get third party to cover risk for us, the information of the organisation is a risk and those are the things that we cannot do without having somebody else hedging us against the possibility of that risk.

The other Executive had a differing view his response was:

"We don't have the formal process, I understand you have got a formal process where you know the risk appetite can be identified and defined; we don't have that process. We started our discussion around it as we were trying to service commercial strategy for example, because there is some risk in it, when you deal with the commercial side of the business there is some risk that you need to identify and you will take them knowingly that you know here this is our risk appetite. So like for me, I am not an expert in this area, I understand it because it is part of our discussions, sometimes we do formulate strategies and there is a need for that! But I think the practice you know, we know what risk we will take of course because there is a consultation process".

The company secretary had a different view saying "previously I wouldn't say everybody knew what the risk appetite is, and maybe even as management we would go through the enterprise risk management processes and we identify the top ten risks and we know that as part of the risk management processes the board needs to actually agree or approve or set the risk appetite. They need to be agreeable on what we can say we accept, we can deal with this, we can tolerate this. But previously that has not always come out clear and this year for the first time I think we are very clear on that, maybe because the system that we used for the enterprise risk management review and the process facilitated by a different set of people from the ones that have always facilitated our risk assessment review in the past; because this year we said as management around the system we use, we use very transparent, actually I fell in love with the system that the external auditors assisted us with and by the time we walked out of that session as management, we had almost sort of agreed that this one we can live with, but that still has to be taken to the board level once we have come up with that risk register, our risk management report and register already had **indications of what our levels of tolerance are, our risk appetite is.** So from this year going forward I think we will follow the similar suit as we did with the system; there is some software in the system and *ja,* I think the risk review process was facilitated by our current auditors. We used to use previous auditors but they were using a slightly different approach and this year **we walked out that day with risk tolerance levels and appetite having been made clear at management level and then we took that via the audit committee and it was signed off by the board".**

The CEO agreed with the other Executive that "this is an area where I would say we still have a gap. In fact when we were having our last board meeting, it is one of the issues we have discussed with the board, to say we need as the board to identify our risk tolerance and the risk appetite; **we are not yet there.** However we do the

materiality framework which we use when we are dealing with some of the risk. We look at if this happens that will be catastrophic, and if this happens that will be significant, if this happens it will be medium, and then these are minor issues. But the gap around the materiality framework that we are using is so linked to the revenue that is being generated, that comes in within the organization. So for me it is just not broad enough. But we are using for now the materiality framework. But in areas where there is no policy specifically that is dealing with the issue, that is where the gap is. But in areas where we can insure, we insure".

The risk official also explained that "the board will determine the appetite, because they are the custodians of the risk. Commercial revenue is needed to balance what we are not getting from government so there are competing needs and limited resources. So I would say our appetite will not be that huge".

Is there a point before finalising the strategy where you can confidently make a statement that says "we have covered whatever possibility we could think of" as far as risk to our objectives are concerned?

A respondent stated, "There is a point where we say yes, these are the key risks that we have covered".

The other interviewee alluded by saying, "Well you can't eliminate all risks, but you can get to a level of comfort, to say that you have covered enough ground".

The other response was, "There is a stage where we feel alright, we have covered all the risks, but they are always concerned that the resources might limit us in mitigating those risks, so we need to monitor them very closely and secondly we must identify areas where we need to be more aggressive".

The company secretary explained that "We do the risk review before the strategy, so by the time we go to strategy we are already basing whatever we are doing on the risk that we have already identified".

The CEO said "When you are dealing with risk management for me it is usually a continuum. Yes, you have got the process of starting identifying the risk but during the year as you look at the controls you have put in place and coming up with a risk management plan from the different divisions, you might find there is something you

have missed and that is then an opportunity for you to go back and look at that. You must remember what we also do is take our risk plan and update the risk committee in more detail now twice a year, for them to look at it. So basically there is an opportunity to re-look at your risk and also when you review your strategy as well".

The ICT official said "theoretically it is possible but as it happened, no not in the strategy session that I was involved in here. So it would be a great thing to have but unfortunately it never works that way, even with guys who pretend that their processes are, I don't think they actually are in that manner".

The risk official view is this "So as a collective we say we are comfortable that at this moment we have this level of predictability in the foreseeable future, this is what we are confident to document and put pen on paper to say this is how we proceed for now, in the foreseeable future. But eventually, every year we do have to review, that is why we do our reviews. So yes, at a point of rolling out a strategy, we do say we have a strategy, we are confident it is a document that we as a collective have come up with, we are confident it is workable".

Can the risk profile change after formulation during execution? What would happen in that instance?

The one respondent explained that "I think the risk profile can change and it also can be informed by change in the mandate. But change in the way we are supposed to do business. You know, the impact in terms of what we have anticipated and in the first three/six months we see that this is really going in another direction and then we need to look at that and see what are the interventions we are going to come up with, and then how are we going to inform our shareholder in terms of really what would have caused the change. Did it come with resources, in which case it will be really adjustment and us reporting and not necessarily major changes; but if it is something that caused major changes it means it has to be effected and taken to the board, the board being informed about it, and if we have any improvements in terms of how we deal with that then give direction, because they are supposed to give direction to the organisation. And then we will factor that in in terms of how we deal with that".

The other view was that "The amount of activities that we execute to mitigate or avoid or manage the risk must have an impact in terms of the level of that risk. You see when

you first identify the risk it will ordinarily be on a high risk profile, and then as we implement activities, and in controlling that risk or even managing that risk with whatever way you choose to manage your risk, the risk lessens; it is either eliminated completely, or it becomes moderate. Or you even probably, the possibility of it happening, the likelihood if it was 90%, you even manage that component and then it becomes 50%. And so those particular changes that are the function of the execution of certain activities on identified risk are in themselves enablers in changing the risk profile of the organisation".

The risk official explained that "the risk profile is almost a final product of the risk formulation. So after that risk register has been collated, it is there and then we profile it, we rate the risks and profile them, and obviously during the course of time the risk profile may change because there will be certain control measures, and they may reduce either the impact or the likelihood of the risk and then that brings adjustment to the final rating of the particular risk and that will mean that maybe where it was a high risk it will maybe go to medium or even low risk, you know, and it even may get to a point where we feel that this risk is no longer a risk. So yes, if you are looking at after control measures have been implemented and the risk has been treated, the profile will eventually change. In fact the whole point is for that profile to change, you want it to change, because we must treat that risk, it must not remain the same level".

How often is the review of the organisational strategies performed to align to the ever changing internal and external risks to the achievement of objectives?

The response was that the strategy is reviewed annually. It used to be three years, but now it is about five year- strategy plan from about two or three years ago we changed to five years. It is also a mandatory requirement from treasury also it is five year period for a strategy.

The other interviewee said that "you do it on a yearly basis, however in reviewing it, there will be quarterly feedback on progress, it is a compliance issue; it is done quarterly where you look at where you are and the implementation of the activities. It is also at that time where you will be looking at your profile and at your risk and seeing what impact they have on the implementation of your program. So I will say formally it is yearly but on day-to-day activities of the organization, when we implement a strategy

we review it on a quarterly basis, we take account of the risk activities that were emerging".

The company secretary simply said "is the PFMA requirement; if you are talking the organisational strategy".

The CEO explained that "we review our strategic objectives on a yearly basis. But it does not mean when there is another risk we need to go back and review the strategy".

What are the specific steps involved during a review of the strategies formulated and implemented?

The one understanding was that "Well we look at the portfolio of evidence in terms of the achievement of milestones".

The other view was that "I am not sure about the steps, but what we do is we look at our annual performance plan and we look at the strategy and then we look as to how far we have implemented the strategy".

The other respondent said "we look at the purpose, whether it is still relevant and then we look at the scope and the vision, the mission. So we look at those steps and then the strategic objectives and then the key indicators, activities. So we look at those steps but you use a certain business model to do those strategy".

The company secretary explained that "there are guidelines and reporting requirements from the national treasury, over and above between us and our shareholder, then we have even the accolade, they call it the Dear protocol for public entities that report to them, we have that document that also spells out what entities are expected to submit. So for us it is a process that starts with the risk management that fits in review, that fits into the review of the strategy by management, from management, management will do its own homework and say to the board 'this is what we think, we have reviewed within the system, here we think we need to adapt slightly and or maybe we think this is no longer necessary for us to keep at a corporate strategy level, we are dropping this to the operational level'. And the board says yay or nay, it goes to the shareholder and like I am saying the process from the shareholder, it is a standard process: you submit the first drafts in August, and then anticipate feedback from the shareholder, sometimes it comes and sometimes it doesn't, and *ja*. But ideally when we submit in

August they are supposed to give us feedback for our first drafts so that if there are changes required we incorporate those changes before November because in November from compliance and reporting requirements, we have to submit the second draft and then the final version in January. After the final version, the board will approve the final version in January but then approval is at an entity level; the other approval, maybe the board will endorse subject to final approval. But by the time you submit the last version in January you are not anticipating any hassles from the shareholder because they have seen the first and second draft and also there haven't been any significant changes since that time – at least in the time I have been here. I once submitted the first draft, the difference between the first and the final draft will be very minimal, sometimes it will be a question of saying maybe in the final, with the other years, maybe the other documents, the other performance players, will have the annual targets but not the quarterly targets. So with the changes reporting they will say they are okay with the content but as you submit the final version make sure that you have included the quarterly targets as well – those kind of changes".

The CEO explained "we look at the environment and what needs to happen. We also look at the priorities that the government are putting in place, is there a change from the previous year? No. Is there a risk for us not to deliver on what we need to deliver on? Yes / No. Is there an opportunity for us? You know? And what is the risk of not maybe getting that opportunity".

The risk official explained "There is a structure with strategy planning, there is a structured approach; it is always a structured approach where you will begin with what exists, you know you look at the mandate, the organisation, us as a government entity, you look at our mandate, has our mandate changed, you know, and the vision, the mission. Is there a change in that? If we are still happy then we are happy. We move forward. So it is a structured flow of activities, how you treat the strategic review. We review the vision, the mandate, the mission, then you go to your strategic goals or objectives, and eventually you have your frame where your strategy goes, your strategic objectives, and then you put in the key performance indicators to measure them, and time frames and all of that will be in there. So it is also usually facilitated by an objective external facilitator who will not get lost in detail like us internally, where we start debating issues internally. So the facilitator is there to make sure we have followed the structure".

What is the significance and evidence of the enterprise risk during the review process?

The one response was that “It is the strategic document that is a product of that review, because it will be different to the one”.

The other view was that ”first you have a session, strategic or a plan review and then we review that one, and the first evidence will be the register and the minutes and then after that, after the plan or strategy has been finalized, then it will be presented to the EXCO as well as to the board – that is when it gets approved by the board, and then the evidence is signed off by the board”.

The other view was that “one of the initial pages of the strategy document, you also usually find the strategic risks that are listed there, because we have gone through them, because they are guiding principles as well; they form part of the guiding principles to the strategy”.

Does risk management form part of any Key Performance Indicators or job profiles at any level in the organisation?

The one view was “I think it may not necessarily be written as such. But as individuals at lower levels they may not understand that I am actually contributing to addressing the risk in terms of what I am doing. But at management we know, but also the business continuity calls for you to have that it is also a risk”.

The view expressed was “It is, the manner in which it is captured, in the lower levels it is captured such that it is engrained in the work, their day to day activities”.

The one respondent explained that “from the EXCO level, we have just had our discussion as we were closing the financial year, that we actually need to make sure that at all levels, because we have a feeling that as much as it is in the performance agreement work sheets, we need to improve in sync-ing it. So now it is actually almost at the level, because you get it at EXCO level, senior management level, and your unit level. Where you have got your focus that for example that deals with users, piece stakeholders, they are at very junior level. So we make sure that in their worksheet, at the entry level, it is addressed. we have got our corporate secretary, a person who is

also hosting the risk register, (I know the board wanted us to have that and appointed somebody specifically for that, but we don't) – so I can imagine in her performance agreement it will talk directly to the risk, but ours talks to related activities or programmes".

The other view was that "especially the risk owner, there is that on the agreement, the performance agreement one of the targets must be the review of the risk and also on those responsible for business continuity plan, it is also on their agreement that it is part of your performance".

The company secretary responded that "maybe KPAs, *ja*, maybe KPAs and KPIs, especially as much as from the policy perspective and the drive to inculcate the culture of risk management throughout the organization, everybody is expected to do their bit at all levels, but at management levels especially, those things that would have come up with the respective general managers for example, and senior managers, are actually expected to ensure that the risk that fall within their respective areas are managed properly – and that is in line with the risk management policy as well. Obviously the detail of what goes into for example the annual performance agreements of different managers would differ according to the level and nature of their job functions, to say how much is expected of them. But at senior management level and okay, let me talk for myself first, because it is not like I go around and review other people's agreements, mine would have that and my expectation is that any other general managers, executive managers' performance agreement has a risk management element in it".

The CEO said "If you look at our strategy itself, no. 1 we need to have e.g. if you look at the strategy and you look at one of our key objectives, it is to have an unqualified audit, clean unqualified audit. And then there is a column that talks about the program activities that need to be there. Risk management is in there, as part of the strategy itself. So when the auditors come and they are looking at auditing us, for us to reach that key performance indicator of having a clean audit, we need to make sure that we manage our risk effectively and efficiently within the organization. So yes, it is linked, and then from there it is going to move to the other levels. But at the moment it is up to the level of the senior management. E.g. I talked to you about the business continuation, so there are objectives for people who are responsible for that".

The other respondent explained that “it would be part of a broader KPI for a manager, called leading and directing your unit, so when you lead and direct that unit you must manage risk as well, within your unit. So it is one of the KPIs”.

The risk official said “well the answer may not really be very clear but the way our performance management system is applied in the organization is such that we try to reflect in the performance agreements, the key imperatives you know, of the division, because they are done divisionally and cascaded down. So from the development manager, his/her performance agreement must address the organisational imperatives, which are enshrined in the strategy and some of them in the risk register as well. Okay. And the people that report to that head of the division, their performance agreements must talk to also to the deliverables of their head, to support the implementation of whatever is in his/her performance agreement – which actually is talking directly to the strategy and the risk register. Then it comes to operational risk, some risk may not be linked directly to the operational divisional head, it may be linked to people below him because they are operational by nature you see. So yes our drive all the time is to tie into the performance management agreements, the important key performance areas. And how do we measure performance? It is not performance of individuals, ultimately the collective performance of individuals must translate to the performance of the organization and that is how our performance management system is structured. So individuals perform, and it must show in the performance of the organisation”.

5.4.1 **Conclusion on Proposition 1 Finding:**

The results pertaining to proposition one as displayed in Table Three are showing that the foremost important step is not completely understood by the officials yet at the top of the public sector institution. The basis of undertaking risk identification is not fully clear yet but there is mostly an understanding of the assessment of the identified risks though it is still entirely facilitated by external service providers as stated by the respondents. The setting up of mitigation plans is well understood as well as the significance of risk profile during the implementation and the review processes of the organisation. The concept of risk appetite in not yet known.

5.5 Research Proposition 2

ERM benefits the organisation in the allocation of resources to capture any opportunities based on a risk management system to create the most efficient method of delivering service to the public.

How exactly does the risk management system affect the allocation of resources being of human or non-human nature in the organisation?

The interviewee outlined that “Because you now talk to the resources: we have identified the risk and the risk register and strategy and so forth, risk policy, and the resources. Now you allocate to say what is to be done these are the resources you need and you also have a column where you report on that, that this is going to be within budget or it requires additional resources and how you go about budgeting for that”.

The other response was “We are not like for instance a laboratory just like any other laboratory; we have a particular science discipline, so that on its own says that more resources have to be given to operations, so that there is a sustainment of our character as an organization. And so operations is where the core staff is, and so in the past, in the slicing of the pie, you basically have to give the larger portion to operations because you are guarding that”.

A respondent explained to say “for example I am busy with a masters system plan, which has identified some skills gap on the ICT that need to be addressed urgently. So the first approach now is just to look, ideally at what resources are needed for this NSP, but what are the urgent matters that need to be addressed, and one of them is to have the operations manager with certain skills at the level lower than the senior manager – but with certain skills, because we need those skills”.

The other interviewee said “Especially the human, when you look at the risk in terms of the staff, we do look at how many people need to be allocated a specific office or specific region or a specific department, and then we will look at how do we normally retain, especially the skilled people, because one of the risks is the retention of the skills, the scientific people. So we do look at that and then try to allocate some resources in terms of retention of those highly skilled people. Non-human, there are

some areas where it requires non-human resources or simple finance in terms of the infrastructure, allocating it in such a way that it might cause a risk for the organisation".

Company secretary expressed the view that "to a certain extent it would affect the allocation of resources, because if you have a standard mandate of what is expected of you but it is not every year that you can be able to do all that you anticipated or needed to do, but after having gone through the risk and assessment process and identified those risks, for arguments' sake, what we have agreed on, even with the risk identification process, where you say for you to mitigate that risk you need to come up with a-b-c-d for activities – **some of those activities will require either email or financial resources. So the extent to which you will be able to mitigate the risk as well is depending on whether you will have the resources available. So as we go through that process we go through that".**

The CEO stated that "the challenge that we have at the moment, is that I don't have enough funds to have a risk officer. So for now we have utilized the resources that we have in-house, the company secretary in terms of our governance".

5.5.1 **Conclusion on Proposition 2 Finding:**

As indicated in Table Three the allocation of resources is completely aligned to the risky areas of the organisation. All officials participating in the research explained that risky areas are always the ones getting the most allocation of available resources.

5.6 Research Proposition 3

Public sector institutions will influence compliance levels by improvement of its strategic risk management systems which manages compliance risks

Please explain to me how the risk management is perceived or confirmed by the organisation to improve on compliance level by both the organisation itself to the laws the institution operate within and to the parties external to the organisation which are served by it i.e. the parties regulated by the institution?

The respondent was clear by saying "It is precisely for that, it is really for compliance, but over and above that it is for you to be able to deliver what you have to deliver with

peace; you identify the risk and you say 'this is what I need to do' but at the end you realize that you had to do that because you also have to comply".

The other official explained by saying "yes, but in terms of other third parties complying with what they are supposed to comply with, there is room for improvement there, by tightening the legislation to be punitive and to have the control platform to do so. I am saying the non-existence of a monitoring tool to ensure compliance for the organization is detrimental not to the organization and also to the national interest, because, it had the potential to cause unnecessary economic downtime".

Again the other official reiterated in saying "That is the strategic objective, it has informed compliance, there are strategic objectives that talk to compliance. It talks both nationally and internationally. And then the compliance is also reflected in the risk register itself, in terms of audit findings. But there are so many compliances that we need to adhere to".

The other interviewee said "It is still a bit complicated for anyone to have a simple answer to, because for example compliance in general would come out of us being a Schedule 3A entity, from the SA Government perspective. But because we are part of the international board as far as we have to comply". The CEO explained "It does in a way because when we look at different risks, identifying those risks, we also look at issues in terms of compliance, our act itself, has given us a responsibility of being authority. So the issue of risk management is part of what we are supposed to do on a daily basis because our job is to protect lives and property even life at sea. So it is also embodied in what we do, in terms of the standards we have set".

The risk officer also summed it up by saying "one of our strategic objectives talks about compliance to international and national legislation and regulation, you know? It is right on top, the strategic level, and I mean that gets translated in various divisions depending on what regulations are affected. So if you talk about compliance it is all over; we all have to comply one way or another to some legislation or some regulation or some regulatory requirement. So by the nature of what we are doing we have to comply, and our products we produce have to comply to those standards. We are in a very sensitive industry, we have to supply a particular product in a way that it is packaged and of a quality that they require. So yes, we have got those demands placed on us. And like I say because it is so important, these are things that define whether we survive or not, and also we don't have, I won't say we have our own

regulations. We do extend certain requirements to our customers or clients, and we extend them like national treasury regulations for instance, PFMA, you know? We will extend them to our service providers. As good management practice and good governance. **So for us the risk management methodology works also for governance, also as a management tool, because it gives us a structure and a way of following through on our matters to the end, so things are not left hanging and then they fall within the cracks and then they pop up one day and you know it becomes a huge threat to the organization.** So it is both for governance, for the management tool – yes. And compliance! Maybe compliance is not even the first thing".

The lack of skills and financing come up as a big part of the problems. Most officials referred to this as being a major factor hampering the immediate implementation of plans but other means are ultimately undertaken after some period.

5.6.1 **Conclusion on Proposition 3 Finding:**

As seen in the summary Table Three, the risk management system has leveraged the compliance levels of the institution to greater heights. All the action plans that have been identified as treatment actions to risks relating to the objectives of the organisation have been turned into strategic objectives which included compliance to all applicable regulations both nationally and internationally.

6 CHAPTER SIX: ANALYSIS OF FINDINGS

6.1 Introduction

The new Companies Act 71 of 2008 (The Act), the King III Report recommendations, and the PFMA (sections 38(1)(a)(i) and 51(1)(a)(i)) (National Treasury, 2010a) have been legislated to ensure that public companies, state owned companies, and any willing private companies, adhere to the best possible governance practices, including transparency. Among those, the requirement for risk management practices, through the risk committee and the risk officer, is specifically stated. Risk management is one of the strategic systems that any organisation can implement to assist in achieving organisational objectives.

This chapter will induce the analysis from the findings presented in Chapter 5. This will be performed against the research propositions presented in Chapter 3. The propositions in Chapter 3 are directly based on the theory in Chapter 2, therefore, a conclusion on whether or not the evidence gathered supports the theory stated in the research, will be provided herein.

6.2 Research proposition 1 Analysis of Finding:

The adoption of Enterprise Risk Management (**ERM**) by an organisation enables the view of **organisation–wide risk** in a systematic method enabling the **formulation**, **execution** and **continued review** of strategy in line with the internal and the external environment of the organisation to minimise strategic risk as defined.

“Risk can be defined as uncertain future events that could influence, both in a negative and a positive manner, the achievement of the company’s objectives (King, 2009). Put in another way, risk is the effect of uncertainty on objectives (Purdy, 2010), meaning whenever there are objectives to be achieved, as every entity exists to achieve certain objectives, there will always be risks to be considered. Nocera (2009) explained that risk is only a risk in a context of an objective, therefore, where there is no objective, there is no risk. This means that the basis of any risk identification, assessment of the identified risks and the mitigation plans to reduce the risks, can only be the objectives of the organisation (see Figure 1 for risk management step by step presentation). von Wangenheim, Silva, Buglione, Scheidt and Prikladnicki (2010), outlined that risk management is a systematic process of identifying, analysing and responding to risk.

The first question relating to the basis of risk management were posed to the Executives in an institution that was used as a case study as per chapter 5. The five Executives, including the CEO and the Company Secretary, were very clear that the mandate given to the organisation as well as the objectives of the entity were the main basis of risk management. The organisational objectives would lead to the risk identification, assessment and mitigation plans to minimise the identified risks as those would be risks to the objectives as set. The one Executive cited the King III requirement being the basis of the risk identification, assessment and mitigation plans being implemented. The other two officials referred to the risk registers as being the basis of performing risk Identification, assessment and mitigation plans to reduce risks. In concluding the responses for this question, it is clear that most of the senior officials at the top level of the organisation have the understanding of what forms the basis of the risk management steps that they perform. But it is also clear that not all the senior officials have the same understanding and insight to be able to articulate and link the basis of the risk management steps to the organisational objectives easily.

In responding to the risk assessment part of question 1, all respondents explained that the risk assessment has been performed with the help of external consultants but there seems to be some understanding, though not a full understanding, of risk assessment. Lyon and Hollcroft (2012) explain the importance of risk assessment being a combination of risk analysis and risk evaluation per Figure 1. The ten pitfalls of not conducting assessment accurately were outlined in Chapter Two.

Risk management is the identification and evaluation of actual and potential risk areas as they pertain to the company as a total entity, followed by a process of either avoidance, termination, transfer, tolerance (acceptance), exploitation, or mitigation (treatment) of each risk, or a response that is a combination or integration (King, 2009). The recognition of a risk environment is critical, followed by steps to correct or eliminate it (Slahor, 2006, p. 32).

At the organisational level, the risks are referred to as strategic risks where the risks are mainly qualitative (Chapman, 2006, p. 287). Gates (2006) also referred to the qualitative risks as “soft risks” but they are significant risks which could be underestimated as they are not clearly quantitative, and they need to be monitored by organisations.

Having set the objectives, the risks to the objectives have also been clarified, the critical point becomes setting up the strategy that will achieve the given objectives while fully embracing the entire risk management methodology both at the strategic and the operational levels of the organisation. The operations plan generally is drawn directly from the strategic plan, the two needing to be aligned.

Slywotzky and Drzik (2005, p.80) have defined strategic risk as "an array of external events and trends that can devastate (an organisation)'s growth trajectory and shareholder value". All senior officials in any organisation need to be fully aware of what the organisational or strategic objectives are, what the risks to those strategies are, why the enterprise-wide risk management system has been implemented, where the implementation has been done, and the basis of the implementation of risk management has to be clear.

Johnson and Scholes (2006, p. 369) indicate that "strategic risk can be seen as the probability and consequences of a failure of strategy". This puts emphasis on the formulation of strategy as being the overarching feature in reaching objectives. This is the question that the executives participating in the research were required to respond to through explaining how the organisational risks are integrated into the formulation of strategies. It came out clearly from all the respondents that the risks to the objectives are the main drivers of strategy. The one executive said this about the strategic objectives: "we then phrase or work out an objective that will be directly responding to that strategic risk identified".

The other respondent then said: "So we do take into account the risk when we do the objectives, because if I look at all the objectives, they are also linked more to the risks". The executives seemed to have a good understanding of the fact that most probabilities of failure of the strategy or strategic risk call for "strategic management" as defined by Bryson and Alston (2011), as "the appropriate and reasonable integration of strategic planning and implementation across an organization (or other entity) in an on-going way to enhance the fulfilment of its mission, meeting of mandates, continuous learning, and sustained creation of public value". These authors submit that there should be continuous learning to enhance the fulfilment of organisational mandates. This is where we talk about ERM as being about taking a holistic, company-wide approach to managing a company's risk, and aggregating information centrally in the organisation regarding various different risk exposures" (Alviniussen & Jankensgard, 2009, p.178).

The difference between risk management and ERM is in the approach to managing risk; where a corporate approach is followed risks are managed centrally and aggregated in the central point in an organisation, but where risks are managed independently of each other, “the latter is usually referred to as the “Silo Approach”, whereas the former is referred to as Enterprise Risk Management (ERM)” (Alviniussen & Jankensgard, 2009, p.187). The key focus of the concept of strategic risk is not on the management of the risks but on the strategy itself as it would have been outlined, a strategy should have taken ERM products into account (Chapman, 2006).

The significance of ERM as posed to the Executives as a question was clear that it is at the centre of the strategy and all respondents were clear. The company secretary explained that “if you go to any copy of the strategy documents, there won’t be a single one that hasn’t captured the risk, because even the timing of how we go about doing that, we do the enterprise risk management review in the first quarter of the financial year and the strategy in the second quarter or by the time we go to the strategy we have already identified the strategic risk, so there is no way we can leave those out at all”.

The CEO emphasized that “the board takes it very seriously, four or five years ago there wasn’t a risk committee in place, so we realised it is something that is very important for an organisation, so we have put the risk committee”; Lafuente and Desender (2012) demonstrated this through ERM being used as a deterrent for increasing company ratings. Hutto (2009) also states that if an organisation is inhibited in its ability to render services to its clients, or if poor management of its organisational risks takes assets away from the intended purpose, it should be pointed out that risk is not just the actions of one’s self but sometimes stems from the actions of another. The harm of poor risk management practices is felt as evidenced by the disasters in corporate failures, according to Kaplan and Mikes (2013), due to the many disasters and corporate scandals that happened, including Lehmann Brothers, WorldCom and the September 11 event in the USA. The risk frameworks have been designed with the intention of guiding organisations on how to look at all risks and use the framework to have sight of the risks facing the entire organisation from all possible angles. ERM provides a general view from which any harm that can happen to the organisation can be observed (Wiklund & Rabkin, 2009, p.55).

When the respondents were asked whether they as top management of the institution knew how much the organisation is willing to take risks, or the risk appetite of the

organisation, it was very evident that this area is still not yet understood and this is evidenced by the literature. Dey (2012) explains that even though risk management standards are supportive in embarking on risk management processes, they do not benefit to indicate correct tools for risk identification and analysis. In addition, it does not deliver any indication on risk factors/events that might need to be addressed in order to manage risks effectively. The fact that risk management is still emerging and has not reached a maturity stage is based on a ten year field study and over 250 interviews done by Kaplan and Mikes (2013) (Coetzee & Lubbe, 2013).

They therefore suggest that ERM frameworks, principles, guidelines and standards are just not giving the results that are needed. “These references do not give the required specifications of which type of risks exactly needs to be managed”. They therefore suggest that until we can give a complete framework, we should do away with frameworks for now until the ERM ideology is clear and a comprehensive framework can be created. The fact that an organisation still needs to pay a service provider to assist in identifying the risks to the company’s objectives is a clear indication from the case study performed that the risk management frameworks still need to be made more usable by the organisations without external consultants.

Kaplan and Mikes (2013) submit that the theories are inadequate and insufficient because Standards and Guidelines that aspire to be “applicable to all organizations” and “all types of risk”, themselves run the risk of being so general that they lack specific meaning. It is argued by them that prematurely standardizing these concepts and principles of risk management is sacrificing the capacity for innovation which is crucial to an emerging and an open-to-all field such as risk management. The institution needs to be able to create within its normal operations the processes that are suitable for its own functions for the continuous review of risks that may threaten the organisational objectives without too much emphasis on the frameworks.

In the face of the fact that many analysts find this position of standard ERM frameworks unsatisfying (Bonisch, 2012), at this stage of the risk management venture, we can absorb and add by studying risk practices, therefore the different risk management practices need to be studied further. The frameworks as given currently, depend on context and may not always work as they can’t help to identify what is risk, how to assess it, and the action to be taken to mitigate the risk may not be valid.

The small number of field-based studies of ERM indicates a diversity of practices across organisations, in the same industry (Mikes, 2009; 2011) and even within the same organisation (Hall *et al*., 2012; Woods, 2009). Arena *et al*. (2010), undertaking three comparative case studies to detect a constant and developing a collaboration between pre-established management practices and ERM, makes the latter unique to each organisational setting. Due to the complexity of the different risks faced by any enterprise, organisations have put in place different processes and structures in the hope of mitigating and managing those risks (Kaplan & Mikes, 2013).

Notwithstanding this greater focus on ERM, many organisations seem to be disgruntled with the way risk management practices are implemented (CFO Research Services and Towers Perrin, 2008; Beasley *et al*., 2010).

The participants were also asked a question on the change in the risk profile **after** the formulation of the strategy during implementation to assess how this is catered for in the risk management processes of the organisation. The responses indicated the understanding that the re-assessment of risk is critical at this stage post the formulation of the strategy during the implementation and also at a later stage post the implementation being the strategy review point.

6.2.1 **Conclusion on Proposition 1 Analysis of Finding:**

The basis of the process of Risk Identification as stated in the literature review is not equally understood by all senior officials of a public sector organisation used as a case study. Risk identification is the first step in the process of ERM as outlined in Figure 1. This is adopted from the process in ISO 31000 standards and this is the first step that needs to be clear to anyone embarking on a risk management process. The assessment of the risks and the ten possible pitfalls when a risk assessment is conducted, as outlined in the literature review, is critical. The fact that the services of an external consultant have been employed shows the commitment to learning the process by the public sector institution and to creating an accurate assessment of risks. The development and implementation of action plans is a step well understood by the officials concerned such that the actual risks to the objectives have been converted into strategic objectives implying that the strategies to reach objectives are the same steps to dealing with the risks to the organisational objectives. This clarifies the responses to the questions relating to the significance of risk when the

formulation, the execution and review of strategy is undertaken. The formulation of strategy is directly based on the identified risks to the objectives of the organisation.

During execution or implementation of the strategies, risk is again put at the top to ensure that the main risks to organisational strategy are always mitigated as much as possible. Again when the strategy review sessions are conducted, the main risks are reviewed in ensuring that the strategies being followed are still relevant. In line with what the literature revealed, though the institution with the help of the external consultant is doing its best to align itself to the risk management frameworks, it is critical that the organisation find its own routine in line with its operations to entrench risk management into the daily undertakings of business, and risk management must not be seen as a standalone activity.

6.3 Research Proposition 2 Analysis of Finding

ERM benefits the organisation in the allocation of resources to capture any opportunities based on a risk management system to create the most efficient method of delivering service to the public.

All the respondents were clear that the allocation of the resources is hugely informed by the processes of risk management as it would have been recorded and clarified where the main risks are to be managed (Power, 2012; Kaplan & Mikes, 2012). This is supported by the theory in the literature review and it clarifies the fact that this may be one of the most important products of the implementation of ERM as returns on investments in assets are maximised (Hoyt & Liebenberg, 2011).

6.3.1 **Conclusion on Proposition 2 Analysis of Finding:**

The allocation of resources is influenced by the risk management system, and therefore resources are indeed allocated in relation to where the main risks have been identified.

.

6.4 Research Proposition 3. Analysis of Finding

Public sector institutions will influence compliance levels by improvement of its strategic risk management systems which manages compliance risks.

ERM has the effect of ensuring that all the risks that need to be constantly monitored are indeed kept under continuous examination (Hoyt & Liebenberg, 2011).

The response by the risk officer also summed it up: “one of our strategic objectives talks about compliance to international and national legislation and regulation, you know? It is right on top, the strategic level, and I mean that gets translated in various divisions depending on what regulations are affected. So if you talk about compliance it is all over; we all have to comply one way or another to some legislation or some regulation or some regulatory requirement. So by the nature of what we are doing we have to comply, and our products we produce have to comply to those standards. We are in a very sensitive industry; we have to supply a particular product in a way that it is packaged and of a quality that they require. So yes, we have got those demands placed on us. And like I say because it is so important, these are things that define whether we survive or not, and also we don’t have, I won’t say we have our own regulations. We do extend certain requirements to our customers or clients, and we extend them like National Treasury regulations for instance, PFMA, you know? We will extend them to our service providers. As good management practice and good governance. **So for us the risk management methodology works also for governance, also as a management tool, because it gives us a structure and a way of following through on our matters to the end, so things are not left hanging and then they fall within the cracks and then they pop up one day and you know it becomes a huge threat to the organisation.** So it is both for governance, and for the management tool

6.4.1 **Conclusion on Proposition 3 Analysis of Finding:**

The risk management system has indeed influenced the compliance levels by elevating compliance to new heights, as explained by all participants to the research. The fact that compliance to regulations was identified as a risk to achieving some of the objectives of the institution assisted the development of a strategy within the risk management system that was directly aimed at ensuring that compliance to national and international regulations is always upheld.

6.5 Introduction

The objectives of this study were to gain insight into the risk management system within public sector institutions, to understand how the ERM frameworks are being applied within public sector organisations, and to compare the current application to what the current literature suggests. This chapter highlights the main findings of the study undertaken and the recommendations to the various stakeholders will be outlined.

Extensive literature has already been generated in some industries in relation to what the ERM frameworks are meant to achieve. The objective of this study was to make insights available into how the ERM frameworks can be made usable and be a critical management and strategic tool within the operations of a public sector institution.

6.6 What questions were asked at the commencement of this research?

The general perception and actual performance of organisations in the public sector has always been unsatisfactory and subject to criticism from both the society and the private sector in South Africa. There are still some very competitive institutions that are ranked among the top globally including the Reserve Bank of South Africa and the South African Revenue Services being the researcher's employer but more understanding is needed to create stronger public institutions.

Organisations that do not achieve their stated objectives can significantly increase their chances of succeeding if the strategies that are formulated are continually reviewed in line with the ever changing environment that we currently manoeuvre in daily. The Public Sector Risk Management Framework was released in 2010 by the National Treasury requiring all public organisations to implement the principles of the framework in order to assist in strategy formulation and implementation. ERM takes a holistic company-wide management of risks to effectively manage exposure to risk.

Due to the fact that academic literature on risk management has only being formulated in the past two decades and few case studies have been conducted, a case study was undertaken within a public sector institution. The findings based on individual propositions are outlined below. The main observation is that precision is still needed

for the senior management teams in how to use the current operational processes to manage risk within public sector.

At the inception of this research the following were the questions the researcher stated:

- How do public sector organisations or agencies utilised by the government achieve government's goals and determine their business or strategic risks, operational risks as well as compliance risks in a formal structured methodology as prescribed by Public Finance Management Act, King Code of Corporate Governance for South Africa 2009 Report, and Public Sector Risk Management?
- How does the risk management system as determined above get embedded into the most efficient method of delivering service to the public, leading to compliance levels increasing and managing of external risk?

6.7 What propositions were brought forward after the Literature Review?

6.7.1 **Proposition 1:**

The adoption of ERM by an organisation enables the view of the organisation–wide risk in a systematic method enabling the formulation, execution and continued review of strategy in line with the internal and the external environment of the organisation, to minimise strategic risk as defined.

The basis of the formulation of a strategy specifically taking into account the risk management process in Table 1, wherein risk is identified, analysed and assessed, then action plans put in place, was investigated. This needs to be performed during strategy formulation, implementation and review to ensure continuous monitoring of organisational risks.

6.7.2 **Proposition 2:**

ERM benefits the organisation in the allocation of resources to capture any opportunities based on a risk management system to create the most efficient method of delivering service to the public.

The research determined whether indeed in a public sector institution ERM assisted to direct the limited resources into areas where the need was critical.

6.7.3 **Proposition 3:**

Public sector institutions will influence compliance levels by improvement of its strategic risk management systems which manages compliance risks.

The research determined whether indeed, in a public sector institution, ERM assisted to ensure that all rules that need to be complied with are indeed complied with by the institution concerned.

6.8 Major Findings in response to the research propositions

The results of this research have been outlined in Chapter Five and discussed in Chapter Six. The major findings of this research were as follows:

6.8.1 **Proposition 1 Conclusion**

To adopt ERM, an organisation needs the view of the organisation–wide risk in a systematic method, enabling the formulation, execution and continued review of strategy in line with the internal and the external environment of the organisation, to minimise strategic risk. First and foremost in creating an organisation-wide "risk register", as was referred to by the officials interviewed, an organisation in the public sector exists to fulfil a specific purpose as would have been mandated by the national government of the country. Therefore the objectives of the institutions are the drivers that would form the basis of the process of identifying risks as these will be risks to organisational objectives. It emerged that the basis of identifying risks was not always clear to all officials of a public sector institution that was the subject of the research. Determination of objectives is the first step as seen in the risk management process of Figure 1, followed by risk identification.

When the risks have been identified they have to be assessed. All officials related the assessment process to the service provider who assists in this regard and could not independently clarify what an assessment at its core should or should not entail. The literature described the pitfalls to be avoided when risk assessment is being undertaken, as this an important step in the risk management process. Failure to understand an organisation's acceptable risk level was pointed out as one of the pitfalls, as was agreed by most officials that this area still needs to be clarified by the organisation. Communication throughout the assessment was also noted as a key factor among the pitfalls to a good risk assessment. It was clear that only the top level of the organisation has a full understanding at this stage of all the factors of the risk

management process, whereas they should be understood at all levels, all the time, for a full implementation of ERM to be effective.

The action plans that are put in place, based on how the risks have been assessed, are generally converted into strategies on dealing with all the major risks to the organisational objectives. This becomes the formulation of strategies as informed by the organisational risks to organisational objectives.

During the implementation of strategies, the strategies also get formally reviewed and all risks as captured during formulation of the strategy are reviewed following a step by step process also conducted by the external service provider according to the data obtained from the organisation. This leads to a continuous process of aligning the strategies to the ever-changing internal and external environment surrounding the institution, thereby minimising strategic risk as the proposition had stated.

6.8.2 **Proposition 2 Conclusion**

ERM has been the main driver in indicating which areas of the organisation in totality will mostly benefit should the organisation allocate most of its resources to it. All of the officials who were participating in this research explained this by stating that the Executives at a high level, based on the total view of the risks facing the organisation, were able to even let go of their budgets to give financial assistance to the areas where the need was the greatest within the organisation. The risk information that provided data to influence decision making relating to resource allocation, had its source in the enterprise-wide risk registers. In this way, a risk management system created the most efficient method of delivering service to the public within this institution. Management is able to make risk informed decisions not only benefiting one section of the organisation, while the other sections are left worse off, but decisions benefiting the organisation in total when resources are being allocated.

6.8.3 **Proposition 3 Conclusion**

Public sector institutions will improve compliance levels through strategic risk management systems. Any public sector institution is regulated by some or other law to ensure that whatever processes and procedures are undertaken are in the best interests of the public funds and no fruitless and wasteful expenditure occurs. The ERM will certainly indicate all kinds of risks that the organisation is exposed to whether or not those risks are under the control of the institution. Compliance risk is monitored through

the risk management system, and this ensures that no rule or regulation will ever be missed by error as it becomes part of the strategic objectives.

6.9 Recommendations

6.9.1 Recommendation for risk officers in the public sector:

- Roles and responsibilities pertaining to risk, specifically the Risk Officer, is vital. The role will be responsible for ensuring that the risk information from every sector of the organisation is always current and available to feed into any decision that needs to be taken. This will also assist with the continuous alignment of strategic objectives and it does not have to be an event for reviewing strategy but becomes part of business operations. There has to be continuous communication relating to the risk profile of the organisation
- A system, preferably an electronic one, that draws information from every section of the business on a continuous basis, is necessary. This way the information is always current and all top organisational risks can be made known at any point in time.
- The risks strategy and policy document needs to be clear and categorically state what the organisational risk appetite is, and how it should be applied.
- Every step of the risk management plan has to be thoroughly understood by all the management roles in the organisation, for them to communicate it as well.
- A risk culture has to be embedded into the corporate culture such that risk management competencies are recognised and rewarded. The behavioural attitudes will go a long way than just implementing ERM and expecting it to succeed.

6.9.2 Recommendations for future academic research

- Further case studies need to be undertaken wherein various public sector institutions are compared and more analysis can be done.
- All levels of management, from the lower levels to top levels, need to be part of the participants to the research, in order to obtain views from different levels of the organisation.
- Specific processes that can be used for the risk management agenda within the current business systems in the public sector should be researched to ensure

that risk management becomes are part of the daily functions, and are not seen as an added extra by the organisation.

7 REFERENCES

\vSpa\vcek, D., & Malỳ, I. (2010). E-Government evaluation and its practice in the Czech Republic: challenges of synergies. *The NISPAcee Journal of Public Administration and Policy*, *3*(1), 93–124.

Adams, M., Lin, C., & Zou, H. (2011). Chief executive officer incentives, monitoring, and corporate risk management: Evidence from insurance use. *Journal of Risk and Insurance*, *78*(3), 551–582.

Aguilera, R. V., & Cuervo-Cazurra, A. (2004). Codes of good governance worldwide: what is the trigger? *Organization Studies*, *25*(3), 415–443.

Akgün, A. E., Keskin, H., & Byrne, J. (2012). Organizational emotional memory. *Management Decision*, *50*(1), 95–114.

Alm, J. (2012). Measuring, explaining, and controlling tax evasion: lessons from theory, experiments, and field studies. *International Tax and Public Finance*, *19*(1), 54–77.

Alviniussen, A., & Jankensg\aard, H. (2009). Enterprise Risk Budgeting-Bringing Risk Management into the Financial Planning Process. *Journal of Applied Finance, Spring/Summer*.

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organizations and Society*, *35*(7), 659–675.

Arena, M., Arnaboldi, M., & Azzone, G. (2011). Is enterprise risk management real? *Journal of Risk Research*, *14*(7), 779–797.

Bainbridge, S. (2009). < I> Caremark</I> and Enterprise Risk Management. *UCLA School of Law, Law-Econ Research Paper*, (09-08).

Baldwin, R., & Black, J. (2008). Really responsive regulation. *The Modern Law Review*, *71*(1), 59–94.

Beasley, M., Branson, B., & Hancock, B. (2009). ERM: opportunities for improvement. *Journal of Accountancy*, *9*, 28–32.

Beasley, M. S., Branson, B. C., & Hancock, B. V. (2010). Are You Identifying Your Most Significant Risks. *Strategic Finance*, *92*(5), 29–35.

Bernstein, P. L., & Bernstein Peter, L. (1996). *Against the gods: The remarkable story of risk*. Wiley New York.

Bier, V. M., & Lin, S.-W. (2013). Should the Model for Risk-Informed Regulation be Game Theory Rather than Decision Theory? *Risk Analysis*, *33*(2), 281–291.

Black, J., & Baldwin, R. (2010). Really responsive risk-based regulation. *Law & Policy*, *32*(2), 181–213.

Black, J., & Baldwin, R. (2012). When risk-based regulation aims low: A strategic framework. *Regulation & Governance*, *6*(2), 131–148.

Bonisch, P. (2012). An agenda for improving corporate risk management. *the risk debate*. Retrieved October 12, 2013, from http://paradigmrisk.wordpress.com/2012/10/31/an-agenda-for-improving-corporate-risk-management/

Borgelt, K., & Falk, I. (2007). The leadership/management conundrum: innovation or risk management? *Leadership & Organization Development Journal*, *28*(2), 122–136.

Braithwaite, J., Walker, J., & Grabosky, P. (1987). An enforcement taxonomy of regulatory agencies. *Law & Policy*, *9*(3), 323–351.

Bryson, J. M., & Alston, F. K. (2011). *Creating Your Strategic Plan: A Workbook for Public and Nonprofit Organizations* (Vol. 3). Wiley. com.

CFO Research Services and Towers Perrin. (2008). Financial Crisis Spurs CFOs to Weigh Risk Management Practices. Retrieved October 12, 2013, from http://www.insurancejournal.com/news/national/2008/10/01/94218.htm

Chapman, R. J. (2006). *Simple tools and techniques of enterprise risk management*. John Wiley & Sons Chichester.

Clarke, R. (2012). The Challenging World of Privacy Advocacy. *Technology and Society Magazine, IEEE*, *31*(4), 29–31.

Coetzee, G., & Lubbe, D. (2013). The risk maturity of South African private and public sector organisations.

Committee of Sponsoring Organizations of the Treadway Commission. (2009). *Strengthening Enterprise Risk Management for Strategic Advantage*. Retrieved from http://www.coso.org/

Cooper, T. (2010). *Strategic risk management in the municipal and public sector* (Research). Memorial University.

De Vries, M., & Nemec, J. (2013). Public sector reform: an overview of recent literature and research on NPM and alternative paths. *International Journal of Public Sector Management*, *26*(1), 4–16.

Denhardt, J. V., & Denhardt, R. B. (2011). *The new public service: Serving, not steering*. ME Sharpe.

Desender, K., & Lafuente, E. (2011). The Relationship Between Enterprise Risk Management and External Audit Fees: Are They Complements or Substitutes? *RISK MANAGEMENT AND CORPORATE GOVERNANCE, Jalilvand & Malliaris, eds., Routledge*.

Desender, K., & Lafuente, E. (2012). The role of enterprise risk management in determining audit fees : complement or substitue. In *Risk management and corporate governance. - New York [u.a.] : Routledge, ISBN 978-041-587-970-5. - 2012, p. 5-27*.

Dey, P. K. (2012). Project risk management using multiple criteria decision-making technique and decision tree analysis: a case study of Indian oil refinery. *Production Planning & Control*, *23*(12), 903–921.

Drechsler, W., & Natter, M. (2012). Understanding a firm's openness decisions in innovation. *Journal of Business Research*, *65*(3), 438–445.

Drummond, J., & BARROS-PLATIAU, A. F. (2006). Brazilian environmental laws and policies, 1934–2002: a critical overview. *Law & Policy*, *28*(1), 83–108.

Eggers, F., Hansen, D. J., & Davis, A. E. (2012). Examining the relationship between customer and entrepreneurial orientation on nascent firms' marketing strategy. *International Entrepreneurship and Management Journal*, *8*(2), 203–222.

Ellul, A., & Yerramilli, V. (2013). Stronger risk controls, lower risk: Evidence from US bank holding companies. *The Journal of Finance*.

Feller, J., Finnegan, P., & Nilsson, O. (2010). Open innovation and public administration: transformational typologies and business model impacts. *European Journal of Information Systems*, *20*(3), 358–374.

Fowler, T. (2012, November 15). BP Slapped With Record Fine. *Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10001424127887324556304578120140555122104.html

Fraser, J., & Simkins, B. (2009). *Enterprise risk management: Today's leading research and best practices for tomorrow's executives* (Vol. 3). Wiley.

Gates, S. (2006). Incorporating strategic risk into enterprise risk management: A survey of current corporate practice. *Journal of Applied Corporate Finance*, *18*(4), 81–90.

Goverment Accountability Office. (2008). From the Comptroller General. Retrieved October 11, 2013, from http://www.gao.gov/cghome/index.html

Grant, G. (2007). STRATEGIC RISK IS THE MAIN THREAT TO SHAREHOLDER VALUE, BUT TOO MANY FIRMS ARE STILL FAILING TO GRASP THIS NETTLE. *Financial Management (14719185)*, 1.

Gualmini, E. (2008). Restructuring Weberian bureaucracy: comparing managerial reforms in Europe and the United States. *Public Administration*, *86*(1), 75–94.

Hall, M., Mikes, A., & Millo, Y. (2012). How Do Risk Managers Become Influential? A Field Study of Toolmaking and Expertise in Two Financial Institutions. *A Field Study of Toolmaking and Expertise in Two Financial Institutions (April 9, 2012)*.

Harrison, K. (1995). Is cooperation the answer? Canadian environmental enforcement in comparative context. *Journal of Policy Analysis and Management*, *14*(2), 221–244.

Hawkins, K. (1984). Environment and enforcement: Regulation and the social definition of pollution.

Hawkins, K. (1991). Enforcing Regulation-More of the Same from Pearce and Tombs. *Brit. J. Criminology*, *31*, 427.

Heyneke, PE. (2010). *Application of enterprise risk management models during new business development* (Master'sThesis). Potchefstroom - North-West University, 123.

Hill, S. (2001). APrimer ON RISK MANAGEMENT IN THE PUBLIC SERVICE. Retrieved from http://publications.gc.ca/collections/Collection/SC94-118-2001E.pdf

Hood, J., Asenova, D., Bailey, S., & Manochin, M. (2007). The UK's prudential borrowing framework: a retrograde step in managing risk? *Journal of Risk Research*, *10*(1), 49–66.

Hope Sr, K. R., & others. (2013). Managing the Public Sector in Kenya: Reform and Transformation for Improved Performance. *Journal of Public Administration and Governance*, *2*(4), Pages–128.

Hopkins, M. M., & Nightingale, P. (2006). Strategic risk management using complementary assets: Organizational capabilities and the commercialization of human genetic testing in the UK. *Research policy*, *35*(3), 355–374.

Hoyt, R. E., & Liebenberg, A. P. (2011). The value of enterprise risk management. *Journal of Risk and Insurance*, *78*(4), 795–822.

Huarng, K.-H., Mas-Tur, A., & Yu, T. H.-K. (2012). Factors affecting the success of women entrepreneurs. *International Entrepreneurship and Management Journal*, *8*(4), 487–497.

Hutto, J. C. (2009). Risk Management in Law Enforcement: A Model Assessment Tool. Retrieved from https://digital.library.txstate.edu/handle/10877/3658

Jackson, P. M. (2013). Debate: Fraud risk management in the public sector. *Public Money & Management*, *33*(1), 6–8.

Johnson, G., Scholes, K., & Whittington, R. (2008). *Exploring corporate strategy: Text and cases*. Pearson Education.

Kagan, R. A., & Scholz, J. T. (1980). The “criminology of the corporation” and regulatory enforcement strategies. In *Organisation und Recht* (pp. 352–377). Springer.

Kallman, J. W., & Maric, R. V. (2004). A Refined Risk Management Paradigm. *Risk Management*, 57–68.

Kaplan, R. S., & Mikes, A. (2012). Managing risks: a new framework. *Harvard Business Review*, *90*(6), 48–60.

Keynes, J. M. (1937). The general theory of employment. *The Quarterly Journal of Economics*, *51*(2), 209–223.

King, M. (2009). *King code of governance for South Africa 2009*. Institute of Directors in Southern Africa, Parklands.

Knight, K. W. (2010). AS/NZS ISO 31000: 2009-the New Standard for Managing Risk. *Keeping good companies*, *62*(2), 68.

Lederman, D., Mengistae, T., & Xu, L. C. (2013). Microeconomic consequences and macroeconomic causes of foreign direct investment in southern African economies. *Applied Economics*, *45*(25), 3637–3649.

Lo, C. W.-H., & Fryxell, G. E. (2005). Governmental and societal support for environmental enforcement in China: an empirical study in Guangzhou. *Journal of Development Studies*, *41*(4), 558–588.

Lyon, B. K., & Hollcroft, B. (2012). Top 10 Pitfalls & Tips for Improvement. *Professional Safety*, *57*(12), 28 – 34.

May, P., & Winter, S. (2000). Reconsidering Styles of Regulatory Enforcement: Patterns in Danish Agro-Environmental Inspection. *Law & Policy*, *22*(2), 143–173.

McAllister, L. K. (2010). Dimensions of enforcement style: Factoring in regulatory autonomy and capacity. *Law & Policy*, *32*(1), 61–78.

McComb, S. A., Kennedy, D. M., Green, S. G., & Compton, W. D. (2008). Project team effectiveness: the case for sufficient setup and top management involvement. *Production Planning & Control*, *19*(4), 301–311. doi:10.1080/09537280802034059

McDonald, C. (2010, April 26). Few Firms See Themselves As “Advanced” On Use Of Enterprise Risk Management. *Property Casualty 360*. Retrieved October 7, 2013, from http://www.propertycasualty360.com/2010/04/26/few-firms-see-themselves-as-advanced-on-use-of-enterprise-risk-management-

McGee, M. W. (2005, November 1). Measuring the payoffs of strategic risk management. *The Free Library*. Retrieved October 6, 2013, from

http://www.thefreelibrary.com/Measuring the payoffs of strategic risk management.-a0142620212

McShane, M. K., Nair, A., & Rustambekov, E. (2011). Does enterprise risk management increase firm value? *Journal of Accounting, Auditing & Finance*, *26*(4), 641–658.

Mikes, A. (2009). Risk management and calculative cultures. *Management Accounting Research*, *20*(1), 18–40.

Mikes, A. (2011). From counting risk to making risk count: Boundary-work in risk management. *Accounting, Organizations and Society*, *36*(4), 226–245.

Mikes, A., & Kaplan, R. S. (2013). *Managing Risks: Towards a Contingency Theory of Enterprise Risk Management*. Working Paper 13-063, Harvard Business School.

Nakata, C., & Im, S. (2010). Spurring Cross-Functional Integration for Higher New Product Performance: A Group Effectiveness Perspective*. *Journal of Product Innovation Management*, *27*(4), 554–571.

National Audit Office. (2011, June). Managing risks in government -. *National Audit Office*. Retrieved October 10, 2013, from http://www.nao.org.uk/report/managing-risks-in-government/

National Treasury. (2010a, April 1). PUBLIC FINANCE MANAGEMENT ACT NO. 1 OF 1999. *National Treasury of South Africa*. Retrieved October 10, 2013, from http://www.treasury.gov.za/legislation/PFMA/act.pdf

National Treasury. (2010b, April 1). Public sector risk management framework. *National Treasury of South Africa*. Retrieved October 10, 2013, from http://www.treasury.gov.za/

Nemec, J. (2010). New public management and its implementation in CEE: what do we know and where do we go?

Nocera, J. (2009). Risk mismanagement. *Risk*.

Paape, L., & Speklè, R. F. (2012). The adoption and design of enterprise risk management practices: An empirical study. *European Accounting Review*, *21*(3), 533–564.

Pagach, D., & Warr, R. (2011). The characteristics of firms that hire chief risk officers. *Journal of Risk and Insurance*, *78*(1), 185–211.

Parry, M. E., Ferrín, P. F., Varela González, J. A., & Song, M. (2010). PERSPECTIVE: Cross-Functional Integration in Spanish Firms. *Journal of Product Innovation Management*, *27*(4), 606–615.

Peccia, T. (2001). Designing an operational risk framework from a bottom-up perspective. *Mastering RiskVol. 2: Applications*.

Piercy, N., Phillips, W., & Lewis, M. (2012). Change management in the public sector: the use of cross-functional teams. *Production Planning & Control*, (ahead-of-print), 1–12.

Power, M. (2012). The apparatus of fraud risk. *Accounting, Organizations and Society*.

Purdy, G. (2010). ISO 31000: 2009—setting a new standard for risk management. *Risk Analysis*, *30*(6), 881–886.

Reed, S., & Werdigier, J. (2012, November 16). Despite Accord, Spill Aftermath Shadows BP. *The New York Times*. Retrieved from http://www.nytimes.com/2012/11/17/business/global/despite-accord-spill-aftermath-shadows-bp.html

Romzek, B. S., LeRoux, K., & Blackmar, J. M. (2012). A preliminary theory of informal accountability among network organizational actors. *Public Administration Review*, *72*(3), 442–453.

Ross, D. L., & Bodapati, M. R. (2006). A risk management analysis of the claims, litigation, and losses of Michigan law enforcement agencies: 1985-1999. *Policing: An International Journal of Police Strategies & Management*, *29*(1), 38–57.

Salge, T. O. (2011). A behavioral model of innovative search: Evidence from public hospital services. *Journal of Public Administration Research and Theory*, *21*(1), 181–210.

Saunders, M., & Lewis, P. (2012). Doing research in business and management. *An Essential Guide to Planning Your Project. Harlow: Prentice Hall*.

Saunders, M. N., Saunders, M., Lewis, P., & Thornhill, A. (2011). *Research Methods For Business Students, 5/e*. Pearson Education India.

Schwab, K. (2012). The global competitiveness report 2012-2013. *Geneva, Switzerland*.

Schwartz, J. (2003). The impact of state capacity on enforcement of environmental policies: The case of China. *The Journal of Environment & Development*, *12*(1), 50–Y.

Shimpi, P. (2010, January 25). Financial Crisis Exposes Need For All To Adopt Enterprise Risk Management. *Property Casualty 360*. Retrieved October 7, 2013, from http://www.propertycasualty360.com/2010/01/25/financial-crisis-exposes-need-for-all

Simon, W. H. (2010). Optimization and its discontents in regulatory design: Bank regulation as an example. *Regulation & Governance*, *4*(1), 3–21.

Skocpol, T. (1985). Bringing the state back in: strategies of analysis in current research. *Bringing the state back in*, *25*.

Slahor, S. (2006). Manage Those Risks! *Law and Order*, *54*(8), 32–33.

Slywotzky, A. J., Drzik, J., & others. (2005). Countering the biggest risk of all. *Harvard Business Review*, *83*(4), 78.

Tongco, M. D. C. (2007). Purposive sampling as a tool for informant selection.

Treasury, H. M. (2004). The Orange Book: management of risk–principles and concepts. *London: HM Treasury*.

Tshishonga, N., & Vries, M. de. (2011). The potential of south africa as a developmental state: a political economy critique.

Van Rooij, B. (2006). Implementation of Chinese environmental law: regular enforcement and political campaigns. *Development and Change*, *37*(1), 57–74.

Visser, W. (2010). The age of responsibility: CSR 2.0 and the new DNA of business. *Journal of business systems, governance and ethics*, *5*(3), 7.

Von Wangenheim, C. G., Silva, D. A. da, Buglione, L., Scheidt, R., & Prikladnicki, R. (2010). Best practice fusion of CMMI-DEV v1. 2 (PP, PMC, SAM) and PMBOK 2008. *Information and software technology*, *52*(7), 749–757.

Wiklund, D., & Rabkin, B. (2009). The balance-sheet perspective of enterprise risk management.(RISK MANAGEMENT). *Financial Executive*. Retrieved from http://www.highbeam.com/doc/1G1-196312848.html

Woods, M. (2009). A contingency theory perspective on the risk management control system within Birmingham City Council. *Management Accounting Research*, *20*(1), 69–81.

Wu, D. D., & Olson, D. L. (2009). Enterprise risk management: small business scorecard analysis. *Production Planning and Control*, *20*(4), 362–369.

WU, J., MA, L., & YANG, Y. (2012). Innovation in the Chinese Public Sector: Typology and Distribution. *Public Administration*.

Yang, T.-M., & Maxwell, T. A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly*, *28*(2), 164–175.

Yin, R. K. (2003). *Case Study Research: Design and Methods*. SAGE.

Zubcic, J., & Sims, R. (2011). Examining the link between enforcement activity and corporate compliance by Australian companies and the implications for regulators. *International Journal of Law and Management*, *53*(4), 299–308.

8 APPENDIX A: QUESTIONNAIRE

Questionnaire

At Group level.

Opening:

<Greeting and introduction>

I am grateful that you have agreed to participate in this research. I have to repeat that your participation is entirely voluntary and you can withdraw at any time without penalty. In line with normal practice, all data will be kept confidential and used in an aggregated format to protect the identity of participants. If the findings of the research are used in future, this will be for academic purposes only.

I would like you to understand that we are looking for your opinions and perceptions and that your honest answers are very important. Therefore there is no true or false answer.

Kindly note that for purposes of accuracy, completeness or elimination of omission of important details I will record our interview.

Questions:

1 What forms the basis of risk identification, assessment as well as mitigation plans to reduce the identified risks in the organisation?

2. How are the organisational risks integrated and encompassed into the formulation of the strategy or strategic objectives as well as operational plans for the organisation?

3. How significant is the role of “risk concept” when strategy is being formulated?

4. Does the organisation know how much risk it is willing to take, i.e. Risk Appetite and Risk Tolerance? What is this based on?

5. Is there a point before finalising the strategy where you can confidently make a statement that says” we have covered whatever possibility we could think of” as far as risk to our objectives are concerned?

6. Can the risk profile change after formulation during execution? What would happen in that instance?

7. How often can or is the review of the organisational strategies performed to align to the ever changing internal and external risks to the achievement of objectives?

8. What are the specific steps involved during a review of the strategies formulated and implemented?

9. What is the significance and evidence of the enterprise risk during the review process?

10 Does risk management form part of any Key Performance Indicators or job profiles at any level in the organisation?

11. How exactly does the risk management system affect the allocation of resources being of human or non-human nature in the organisation?

12. Please explain to me how the risk management is perceived or confirmed by the organisation to improve on compliance level by both the organisation itself to the laws the institution operate within and to the parties external to the organisation which are served by it i.e. the parties regulated by the institution?

9 APPENDIX B: INTERVIEW TRANSCRIPTIONS

9.1 2013-08-06: 09h00 Interview

So like I explained this is a semi structured interview so I am going to give the question just as an indication but you are allowed to answer it whichever way you feel comfortable and take your time in just explaining the way it is. The more information you give, I am sure the easier for us.

The first question is in terms of, remember my research is I am trying to get the insights into how the public sector do a structured risk management, to say that they have a strategy and their strategic objectives. So how do they in the structured format keep track of what risks are there, to the strategy? So that is the whole thing I am trying to find out.

So my first question, if you don't understand I will just rephrase it, I want to understand what forms the basis of risk identification in your organization, in the way that you understand?

The way I understand the risks for us as an organization is we look at the strategy, we look at the earlier performance plan, we look at the critical things that will impact on our strategy, things that we need to look at to ensure that whatever we set ourselves to do in terms of the strategy and the earlier performance plan, we are able to achieve. So from that, that is really maybe the approach, because out of that is the risk register we look at and then in terms of the goals we have, we align the risk according to the goals and what business they are doing.

Okay, so there are risk registers, so that would form the basis.

There are risk registers, there is a risk management policy and we look at the strategy, and we look at the plan and we look at resources required.

So there is a risk management policy.

Yes, and the risk register. And then our strategy plan, our annual performance plan and we also look at the resources we have to be able to do that.

Ja, so I am going to ask for these documents maybe afterwards, just to see the correlation with the documents. I think at the end because I am sure I will do the

last interview with the CEO and then I will ask for the documents when I collate all the information

Okay, the second one, still on the first question but I am just breaking it down so it is easier to answer, because we have got what forms the basis of the risk identification and now I want to understand how those identified risks gets assessed. In other words to be able to say this is like a low or medium risk, or high impact, or maybe the probability for that one to happen is low, but if it happens the impact will be very high. Like that kind of assessment. How is that done?

There is a way of determining that: we have always engaged with the service provider, may be PWC or whatever, to look at the risks, whether high, medium or low. Then when they do that, the residual or whatever…

But who does that?

The risk register, from there also we take it down to operational levels and then we have a strategy, and we also take it down further but we are just aligning it, because they will identify the key ones that are at a strategic level, but also at operational levels, they must say this is how it impacts the operational levels and we address it like. But the formula is there in terms of how you calculate it – high impact likelihood, and whatever the risk, the metrics that exist. So metrics are done.

Ja, I think that makes sense, when you say at a strategic level and operational level, because I think I get the strategic level is going to be you and the other executives I assume.

Ja.

At the operational level are there specific people who are charged with the responsibility to look into these or how exactly does it work?

At a strategic level it is according to the strategy and NPP, those executives and the senior managers are involved at a strategic level. At an operational level it is now assigned to GMs because out of that you will see this risk is really finance, this is operations, this is communications or whatever. So there are executives who also look at that.

Yes.

And then they align, take it to the departments where a senior manager will look at it and deal with it an operational level. So you have more, maybe you had one, we then unpack and then perhaps you have one at strategic level but at operational level you could be impacted by three or four things, which will be unpacked and they will see how we are going to mitigate it as risk. And begin to report on that and see how we are doing these things.

So let me say what I understand, if I am wrong just let me know: so now there is that strategic risk that will be at the high level.

That's right.

At the operational level, per division, maybe for HR, for marketing, for corporate affairs – every division will have their own risks, which are the ones that will go up to strategy.

Yes.

So now at that division level, maybe at the GM level for HR, they will have based on their own objectives for the division: they will identify their risks and then they will also assess at that level and then come with whatever.

Yes, put in mitigation structures, and how do you end up addressing it and that is what we have to report on, to say we are taking care of this and this is how we are addressing it. At the end of the year you assess whether it is a continuous thing or whether we are done with this part of the risk or whatever.

Hm, because I am sure risk will be changing all the time.

Yes. And the strategy and the resources that you have.

Okay. So I think the last part of question one you also answered, to say that in those divisional risk registers you will have risk, you will assess the risk and you will have mitigation plans.

Yes.

So these mitigation plans from the division would form the basis of the strategy.

How we mitigate that. First they identify at a strategic level and then they come to departmental levels in terms of how we address that. At operational level, it is a departmental level, and we talk to those, how we are addressing them and how we are

mitigating them. And then we report quarterly, because these ones at a departmental level are also being addressed based on the strategy. And then the way we are doing it is if there is anything that we identify which was not covered in the strategy, but we have looked at and it should be in the strategic level.

Yes because I was going to ask you, so you have already answered, because I wanted to say to you when you are identifying at a strategic level, I wanted to ask aren't there others that are emerging, that are identified from the bottom and then rolled up.

Ja.

And then there are others that are identified at the top and taken down.

Yes.

And then depending on what makes more sense and the mitigation and assessment, then others will go up, others will go down.

Yes, because they have been addressed also, and we identify new ones. So it is an ongoing thing in terms of how you want to meet the core of your business.

Okay. So if it is an ongoing thing, because I want to understand that also, because how exactly, how often, what does ongoing mean? Do you say monthly or is there a formal timing that has been set to say that every month we revise this, or…

Ja, we report on risks quarterly.

Quarterly.

There is also the management of that. Remember this is also a body issue, in terms of governance; the risk is an issue, so we have an audit committee that looks at that and reports on that to the board. So at operational or departmental level we are looking at the risks, we review that, it is presented at EXCO – because there is also a risk manager who looks at that – and that is all collated and then it is reported to the sub-committee of the Board, that risk committee, and then to the board. So it is ongoing, in terms of continuously having to review because you cannot continue with the business without looking at the risks that are there that will impact on your business going forward and in terms of the business continuing to management, they need to see for

the business to continue, what are the risks that are there, for us to continue with our business.

So when you say continually, you are saying quarterly. So there is nothing like a monthly risk register from operations?

There is, that is what goes to EXCO meeting.

Okay, so that is what I wanted to get, so there is that monthly, I am sure based also on the monthly you will get the quarterly.

Ja, ja.

That's clear. My question no.2 which somehow I think you have answered mostly: how are the organizational risks integrated and encompassed into the formulation of the strategy or strategic objectives – as well as the operational plans for the organization? So I think that whole rolling up of the risk registers into the strategic level will form the basis of how the risks from the bottom are entrenched into the strategic plan.

Yes.

So that is clear.

So you have the strategic objectives and then you also look now in terms of the risks that are talking to that and you do the risk metrics and you say is it high level or whatever and you assign a number according to the different level and then you say how you are going to address this and who is the risk owner and..

And the due dates maybe.

And I need this to mitigate that, is it going to be within the budget that we have, or are there some additional resources required to mitigate that – and then you do the progress report.

That risk register, because I am sure I will have a copy, I just want to understand for now: it does have a risk owner ne?

Yes, it is with the corporate secretary, who reports to the CEO.

Is it with due dates also?

Ja.

On each risk ne? Say maybe you assessed this particular risk, what maybe 20… it goes to how much?

I think until 20 – or 25 maybe, I can't remember.

25 – something like that.

Yes. 25.

Because I know on a scale of probabilities it is 1 to 5. Also the impact is on a scale of 1 to 5. So I think the maximum will be 25. And then the due dates.

Yes.

But in your knowledge generally do people adhere to those due dates, the divisions?

Ja, I think sometimes people just really think that because we are doing the EPPD and the strategies is for five years, but the risks that would have been identified at a strategic level may not necessarily be up to five years, or it could be up to five years or whatever – but we are now going to measure that every year. So that people who have got a tendency to think that the risk now, we start at the beginning of the financial year maybe up to March, then we put a risk there and how they are going to attend to that, March 2014 or whatever the period. But then in terms of some of the things could be done prior to that, but others would be on goal, but it depends on how you are to function in terms of whether you are allowed in your documentation or management to say ongoing or put a specific date. Because there are those that actually go beyond which will not necessarily fall within: it is a process and it requires certain things that are not within your scope; there are processes you need to follow which do not necessarily fall within a year and if you have not identified something initially and maybe there is a service level agreement, we need to really see what are the issues going into drafting, negotiating, agreeing and then actually saying. So that as an example, may not necessarily be within a year. So there is a tendency to put a date that it must fall within a year, and everything then actually becomes really very suspicious when everything else is March 2014. So you have got to really internalize and I think it just really needs time for the division to really interrogate and say what are the things required within this, so that we can actually put more or less the date where it is reasonable for assessing that kind of risk.

Because for most of the dates that will be set for instance, you say 2014 ne, I would imagine that before 2014, because it doesn't mean that nothing has been done, in the meantime things will be done monthly or whatever, to build up to that 2014. So that progress that is being done gets reported I think in the monthly, to say even if the due date is in 2014, but then..

Yes, it is ongoing.

That makes perfect sense. Question no. 3: how significant, according to your understanding, is the role of risk concept when strategy is being formulated? Like how risk averse or something like that, is the organization – especially when you are formulating the strategy. Is it a big deal really or does it start by wondering what the risks are or just set the strategy and then worry about whatever risks there are, afterwards?

I think it is important really to understand what is it that the organization wants to achieve in terms of the strategy, but you cannot set the strategy without also really looking at the risks, because the critical thing is as much as you want to achieve and you set yourself goals, the first thing is the strategy must talk to resources. Now the first thing you should ask yourself is do you already have these resources? If we are to change, how well are we going to be able to change? Because that change in itself is a risk in terms of managing that change: because if you remain stagnant also it is already a risk, but the fact that the strategy is meant to map a way forward, it already encompasses some kind of procedural risks. So you cannot have a broader strategy without also having the background of the risks. You may not necessarily at that time have identified the risk but in your plan you will already know that there will be some risks. The impact of the risk will then come when we now get to deliver, it will identify the risk in terms of how well we are going to deliver on this. Because delivery or under-delivery is already a risk, so if we over-promise and under-deliver then it is also a risk, but we could over-promise and be able to deliver at that level, where we have identified the risks and be able to say what are the necessary things we need in order for us to deliver.

So in short at the end, are you saying that the risk concept is a big part of certain strategy?

Yes. It is.

Okay. Question 4: Does this organization know how much risk it is willing to take? So in other words, do you, for your own self, have a sense of what is the risk appetite and the risk tolerance, and also if you can just explain the… this is for your own self, so there is no right or wrong answer, so I just want you to tell me according to you, what does the risk appetite for source look like, or what is your understanding of the risk appetite or the risk tolerance, and just explain to me?

I think I understand it well, is that the risk for us, the risk appetite is in terms of mandate. We have a dual mandate, which is the public good and commercial. So our willingness to take on board the mandate we have, says we have a very good understanding of what it is. So in terms of our planning and everything we have a fair understanding of the risk that we have, to be able to meet this mandate – with very little resources sometimes, because with the public good we have to deliver on that, and we also have to go commercial. But the way we are as an agency, we also get additional mandate, sometimes even without funding. So we are willing to take on board those kind of deliveries. So to me it tells me we have a very good in-depth understanding of the risk we are taking as an organization.

So if I had to put it in the words I want to, the risk appetite – would you say the organization has a big appetite for risk taking? Or not.

Yes, we have.

So if they have an appetite for risk it means they take on large risk strategies.

Yes.

Okay, so there is a big tolerance for risk because you take on a lot of risk

Yes, and we sometimes we don't even know how we are going to find it, but we are prepared to swing in and to say what is it that we can do to improve because it is really about continuous improvement and the fact that we are continuously wanting to improve, to really better ourselves and to deliver according to the mandate of the organization, we are always looking at what are the national developmental plans, what are they talking about, what are the certain things that we have not ventured into, how do we go about venturing into that to deliver and to remain relevant. And I always say it is the organization that understands that there are risks that they have to take but at the end, what is it that you have achieved with that? Now we have taken on risks,

global client framework, which we are dealing with, which doesn't necessarily have the funding and it is something we are prepared to take on board and say we want to represent the state on these kind of things and we are now putting together the plans to say 'this is what we will do and this is how much it will need in terms of resources'.

So you are in the aviation side.

Ja.

What are the biggest risks that you have to deal with?

The biggest risk is the expertise I require for aviation, because it is a very high skill that is required to be able to provide the services and then it is the loss of that kind of skill to international bodies, and the risk also is failure, while you are losing that kind of skill, it is not easy to bring in people from the street. It is very specialized, it takes too long to equip a person to where they are actually seasoned and can deliver to what is required, and there is also continuous training that is required in terms of the recommended standards and practices which people providing these services should undergo, and then losing those, or having invested for a long time in that, is something that you cannot…. So the risk is really losing people in aviation, and the second risk is not being able to recover the revenue that the organization or our mother/parent department has ..

But how are you supposed to recover?

We recover through the services we provide. We provide quality services that leads to a standard, we are audited in terms of safety, things that are high risk to safety. So we recover from the services we have provided. But the risk in terms of the state is not to be able to meet certain obligations that are talking to safety; it becomes a risk to the state and globally in terms of our global aviation and how they see these things, and that begins to diminish in terms of the number of flights coming to the country because they are concerned about safety. Otherwise, the other thing is just the liquidation of the airlines because competition is very tough in aviation. So the risk is failure to recover revenue that we have set ourselves to recover and that we want to deliver on the strategy based on the revenue we recover. Failure to recover that revenue means you are unable to deliver certain deliverables.

Okay, so if for instance, what was the airline that went down – 1 Time – say for instance they get liquidated and that is the revenue you are expecting and you might lose the revenue.

Ja.

Shoo, I just think this aviation thing… how many people are in your aviation structure?

At OR Tambo I am having 26 but they are supported by people in the regions because there are also those that are providing services in the regions, so aviation at OR Tambo is actually just over-seeing the regions.

So then all these aviation people have to give the information for weather.

Nationally and globally.

Jo! So what do people have to be really, what specialists are those that have to work, what do I need if I want to come and work in aviation?

You need to have maths, physic, and also specialize in aviation.

Question 5, because for me just the word aviation, I don't know, it is not your normal day to day things you get to speak about. Question 5: Is there a point before finalizing the strategy where you can confidently make a statement that says 'we have covered whatever possibility we could think of as far as the risk to objectives are concerned?'

This question is just saying is it possible that when the executives or maybe yourself, when you come up with a strategy and then you consider all the risks that can come. Can you comfortably at some stage get to a point where you say 'you know, I think we have looked at every possibility as far as risk is concerned' so let's go on with the strategy? Or you can't get to where you say you have considered all the risks?

I think there are many risks, which are identified, but there is a point where we say we are key, but because the risks are emerging, but there is a point where we say these are ten key risks, there is the strategy, because it would have looked at different regions, measured different regions, it would have looked at and said 'this one is new in terms of the ranking, this one is minimal or whatever, it has a low impact, and this

one needs to be removed'. So you give them different rankings, but there is a point where we say yes, these are the key risks that we have covered.

We have covered the keys. So you can get to that stage.

Ja, that is what is covered in the risk register, that is also reviewed.

How much of the external risks that you can't control or are most of the risks within your control?

Not necessarily. If we say insufficient funding, we are talking in terms of the grant that we have and that is external, and also the resources in terms of us having to have initial people that we really need, it is also based on supply/demand, so it is not very easy. Commercial is not within us, because it is how we are going to buy into a product; we have a commercial mandate, how we purchase our products, how we are marketing ourselves, as to whether there will be revenue out of that, that we will generate, and it is also external risks according to whether people buy in, whether we really go out and sell our products. So most of the security is not dependent on us, our instruments are out in the field. So if the instruments are looted and there are a lot of burglary, some of the parts are out in the field! It is also outside of us, we don't have control over these things. So perhaps maybe the guide of how we maintain the instruments ourselves is internal, but in terms of maintenance, there are some maintained but the technology is advancing so much so that is also really outside our control. So there could be internal but external also and we are focusing really mostly on those factors that are external, possibly those that we know we can influence but also those that are more internal really, will be the ones dealt with at operation level. And we address this from within.

Okay. That is clear. No. 6: can the risk change after formulation, during execution, what happens in this instance? So again, some of the questions might seem the same, it is just for academic purposes I still need to ask and make sure: so can the risk profile change? Say for instance you want to set your strategic objectives and you look at everything that might be possible, then you have that risk register that says these are the 15 risks and if we cover them we are good to go. And obviously things change every day so the risk profile, I don't want to answer for you but I imagine the risk profile can change, ne? Or if it can't change you will tell me. But I want to know as it goes when it changes, what are the specific things that you do?

I think the risk profile can change and it also can be informed by changing the mandate. But change in the way we are supposed to do business. You know, the impact in terms of what we have anticipated and in the first three/six months we see that this is really going in another direction and then we need to look at that and see what are the interventions we are going to come up with, and then how are we going to inform our shareholder in terms of really what would have caused the change. So how we go about it is really that kind of process is that either it was mandatory because it came from the shareholder and needed to be done, then it means we have to look at how we are going to factor that, did it come with resources, in which case it will be really adjustment and us reporting and not necessarily major changes; but if it is something that caused major changes it means it has to be effected and taken to the board, the board being informed about it, and if we have any improvements in terms of how we deal with that then give direction, because they are supposed to give direction to the organization. And then we will factor that in in terms of how we deal with that.

But from your side, is it a concern, is it always changing or not really?

Not necessarily. Because I think any changes would have… things could have changed, if when you were formulating your strategy you did not take into consideration some of the mandatory documents that are supposed to be informing the strategy. So you have documents that are mandatory that should actually inform your strategy going forward – much as you want to take into consideration the necessary imperatives and regional development plans – what is the organization seeing, what are the things that we are focusing on and what is our role in any of those. And is there one that we have to report on, is there one that (because they are going to different departments) – but those are the things that actually inform what we do going forward, and there are documents like the Act, documents like the BCE, Basic Conditions of Employment – those are the things that you really usually look at when you do the strategy and based on your mandate what do you do going forward. So anything that changes would be failure of your vision, because you have failed to take into consideration something, and so you formulate the strategy and then you put a risk in, but now the shareholder when you go and present your strategy is the one who says ‘but now what about this thing?’ – which means you have to come back again. But it would have been picked up when you go and present at the beginning, you present to the board and they are happy and give their input and now you go and present to the shareholder, and then the committee, and then they say ‘what about this thing?’ and then you have to come back and no but we have reported this under this item and you have to look into it.

I think it is an advantage because then there are a few committees, a few viewpoints. That is fine. Question 7 you have also sort of answered: how often can or is the review of the organizational strategies performed to align with the ever-changing internal or external risks? So this how often – I guess here I was just looking for if you do have a formal/ informal time frame of reviewing the strategy.

Yeah, the strategy is reviewed annually. It used to be three years, but now it is about five years – from about two or three years ago we changed to five years. It is also a mandatory requirement from treasury also it is five years.

Yes, you come with that five year strategy but then annually you review.

Yes.

I agree that.

Now we have already started reviewing; we started already I think in June/July – because the time frames, there are also set times in terms of reporting, in terms of governance act, there are time frames you need to be submitting this, there is a time frame kept, so we are aware of those schedules in terms of what we do, and what we need to submit and all these kind of things. So it is reviewed annually, and the APPS also.

What is the APPS?

The Annual Performance Plan. It used to be the business plan but now it is the APP.

Okay, so I understand that, I am also happy with that. No. 8: what are the specific steps involved in review of strategies? Are there specific steps when you do your review that needs to be followed?

Ja, I think it varies from organization to organization because throughout the year you are monitoring and reporting on your performance, you have got quarterly reports you are submitting to your shareholder, this would have gone through the different committees and the board, before it goes to the shareholder. Now through your performance in a year you are looking at some, because they are continuously monitoring, you are looking at how well you have done, what are the challenges, what are the emerging things, what are the things that we need to identify now that needs to come into the next financial year's plan or something like that. so you will look at the

challenges, what you have achieved, what are the things you need to really really keep because some of the things you cannot take away because it is something that is talking to the core; but in some of the departments you also say what has been a challenge, what was risk and how do we elevate this into our strategy, and then build it into a strategy. So you would have looked at various things that would have transpired in a year towards achieving what you had set yourself to achieve, and whether you have met the challenges, the successes, the things that ether you have met the challenges, the successes, the things that you are ready to top up and the things you are ready to drop, and really focus on certain areas. Because those that we have seen as just pure operational, maybe you tend to drop those and elevate some of those that we thought were really the challenges and elevate that into the strategy and really move on that, but also keeping the good things you want to keep on reporting on. So we get also the projects, what will be the projects, what is our financial mandate, what is it that we really need to do, or in terms of compliance how well are we complying with different legislation, with the occupational health and safety, what is required in terms of the BCE what are the basic conditions of work and stuff like that, and have we met them, what is the challenge, have we been able to meet our commercial targets and if we have how can we improve it. Those things you look at going forward, to say these are the elements that we need to look at. But I believe at that time the board would also have engaged initially and then to give more or less the direction, by the time risk management come we look at how we have performed, what were the challenges, how we packaged that and then after that to the strategy, to say this is a risk now and how do we address it. We have taken it to the strategy level and we need to deliver. So there is that process. And it also talks to the resources because we should by that time be saying for this we need these regional resources, will we be able to get resources from within the government, how much are they going to give us, how much are you going to commission – which we should also now talk to strategic level. This is the process.

Happiness. Ja. No. 9: what is the significance and evidence of the enterprise risk during the review process? I think this we have covered, ne?

Hm.

Because this question, I was trying to find out what is it that evidence-wise that would be able to show that when we do the review you did look at the risks. So I think all those concerns..

It will be the risk register because it talks to the strategy. If you talk about finance it will be strategic risk, financial, insufficient funds or something. So the register talks to all those things – key strategic goals.

So that will be the risk register for aviation only?

No, the risk register is for the organization.

You don't have your own one that fits into the organization.

We have, original risks – departments.

Yes, yes, yes.

- Which talks to the risk register for the organization which talks to the strategic goals.

And we look at it individually in terms of whether this one is for finance, this is for operations, but you might have one or two lines or anything that you might fit in in the others, but most of the risks will be the ones according to the risk register, they have a risk owner – so if it is operations, if it is financing, corporate affairs. But other departments can just really see this one is going to affect this and finance is going to affect us if we do not deliver on the product. So there is a synergy and an enterprise view in terms of how we go and how things are managed.

Ja, say in your operational risk register, not the strategic one, they have those inter-dependencies, maybe one or two or three of your risks, ne, can only be whatever plan to mitigate it can only be..

Finance, IT…

Yes, so now you will have to what, influence finance to ensure that they sort out..

There are those that are really… the interdependencies is that you will be able to talk to those departments because they also meet at EXCO and you will be able to iron it out there.

Okay, so that is not a big problem.

Ja.

Okay, no. 10..

And at EXCO we also need to find somebody, maybe it is IT, maybe IT and finance need to meet and maybe to talk to SETA about things and so that is how we manage the interdependency and breaking the silos.

Ja. no 10: Does risk management form part of any key performance indicators or job profiles at any level in the organization? Maybe if you can just start from the lowest level, I just want to know if each of the people going up in their KPI's or job profiles there is something that clearly states management as being part of it, or is it just some unwritten thing that everyone does? How does it work?

I think it may not necessarily be written as such, but the understanding of the risk because this is also presented to the staff during the quarterly meetings, you present on your performance in terms of the risk and the controls that are there, the audits, the outcomes of the audit, what the issues were and then you understand all that as risks. But as individuals at lower levels they may not understand that I am actually contributing to addressing the risk in terms of what I am doing. But at management we know, but also the business continuity calls for you to have that – it is also a risk.

Yes.

But at that level, in terms of operationally, they have got to ensure that they do their recovery plans, ensure that they test whatever is in their recovery plans – not that they necessarily understand that this is a risk, but that they are doing the operations; they do that, they have got to ensure that in terms of their work performance sheet, that they have got BCP tests, and they might not necessarily talk to risk because they don't understand, but at the very low, low level they have got the BCP and they have to test those kind of things. And they also have fire things like the occupational health and safety, they are involved as well, they have got to the evacuation and all those kind of things. So but I think they get to the level of that when they say 'we had a weak control here' or 'we had a clean audit, with no matters of emphasis' when she goes around to report on the performance quota. So there is just a little bit of understanding about that. So they understand it in terms of operations.

So from manager's level, senior managers and executives, do they in their KPIs have a specific KPI?

Ja.

From which level?

I think it is recorded at level 12.

So that will be from managers. So the management of risks is part of their KPI's

Ja.

Okay, I have got that one. No. 11: how exactly does the risk management system affect the allocation of resources, being of human or non-human nature in the organization? Is that done according to the risk that is being assessed?

Ja, those were some of the approaches we talked about.

Yes, you did say

Because you now talk to the resources: we have identified the risk and the risk register and strategy and so forth, risk policy, and the resources. Now you allocate to say what is to be done these are the resources you need and you also have a column where you report on that, that this is going to be within budget or it requires additional resources, and how you go about budgeting for that.

Ja, I think you said that before, so this is answered. Okay the last question, I am not sure if we answered this: please explain to me how the risk management is perceived or confirmed by an organization to improve on compliance level by both the organization itself, to the lowest – this is now the lowest level in the organization have to abide by ne- to the institution that operates and to the parties… okay so this question is saying explain how the risk management, how do you perceive this risk management to be impacting on the lowest of the organization itself. Say from where you are sitting, in doing these risk management endeavours, does it help you comply with the laws that you need to comply with? Maybe you have aviation international laws and all sorts of things that you need to comply with. So do you find that when you do the risk management it helps you comply with the laws, or not really.

It is precisely for that, it is really for compliance, but over and above that it is for you to be able to deliver what you have to deliver with peace; you identify the risk and you say 'this is what I need to do' but at the end you realize that you had to do that because you also have to comply. For instance, for us in aviation there are quite a number of recommended standards and practices – by the convention – which we have to do. We have to ensure that we provide a service internationally it is 34 hours; if there is anything that says our IT is not able to run properly, it means we have not done the

risks from IT appropriately, because then we are going to fail in terms of what we need to do. But there is a compliance, we need to say there is data coming in, the data has been quality controlled and we have provided the products according to what is available and there was also an integrity in terms of the systems that we used and the standards, and hence we are certified, because you need to show that there are standards that you have built in to provide international air navigation and that must also talk to the database downstairs in the ICT, the database must comply with certain things – the risk not to run the database according to what is specified in the documents that ACAO has, is a risk. So you need to ensure that you do that and we indicate that the databank must be run according to 123 and you need to report on this at ACAO, some of the sub-structures, and we have got to have back up – failure to have back up procedures is also a risk. And all these kind of things must really work together and be monitored, be reported on and then the quarterly reports, how we do in our tests and stuff like that – to ensure that the business continues. And all those things. And then we are also audited by ACAO over and above the audits, the internal.

ACAO is the international..

Ja, it is the international board that looks after aviation and we have just been audited now from the 24th to 30th of the last month. So we are also audited in terms of the practices and what we do. So it is not just an internal audit here.

So compliance ne?

Ja, you also have to keep doing that. So those kind of risks that are identified and what needs to be done is also what leads us to deliver on the service to the satisfaction of the clients.

Shoo, ja, I think we are done. I am sure I can stop the….

ENDS.

9.2 2013-08-06 11h00 Interview

I have done questionnaires, but it is purely unstructured interview, so the questions are just to guide you on the types of things I am looking for, but it is absolutely up to you how you want to answer, from whatever angle that makes you comfortable.

Okay, so because I have already had the first interview I already have some preconceived ideas.

Who did you interview?

I interviewed …

Oh okay

So I am going to start with the first question: what forms the basis of risk identification within your organization, in your view?

The basis of identification of risk is threefold: it is finance, it is human resources/skills scarcity, as well as preservation of this organization at premier, and scientific institute. And so those are the three major ones; I am not saying the others do not play a role but those are the major ones that play a significant role. If you operate, you look at the institution like ours as the only service provider institute that is of a national nature and that has been accredited on behalf of South Africans, and so there has to be the preservation of scientific knowledge in the organization – that is one key one. And then finances, because ordinarily a government doesn't have an our organization base, so there ought to be a way in which you capture risk such that they make financial sense, and there is a return on investment. As well as the skills base, there is a scarcity of skills, particularly in this segment. It is one of those key factors that we take into account when we are identifying the risk. The other ones are playing a role but not so much because they are mostly operational.

I am going to ask question one but in three separate bits, because I have asked the first part, about what forms the basis of the risk identification. Now I also want to understand how do you assess that identified risk? Say you identify finance as an issue and there will be other risks, so you need to also assess them to say assessment talks about the impact of that risk or the probability of whatever is identified. So how do you then, after you have identified?

We look first at what are the mitigating initiatives that we have, to mitigate the risk or even eliminate the risk, and then look at the prevalence of that particular risk and we also extend to the frequency and the likelihood of that risk happening, without those controls we have put in place. And based on that we assess, on a year to year basis, because also that process is managed by external auditors - well there are internal auditors but we have appointed a firm to actually do that internal audit function. And so they are the ones that actually guide us in terms of the risk management principles, to say that the assessment we have done is an objective assessment and is more or less mirroring exactly relative the organization at the present moment.

Okay, so now we are saying we have identified the risk, we have assessed the risk, so the last part of question 1, the mitigation plans: how are those, how do you come up with the mitigation plans to reduce these identified risks?

The mitigation plan is generated out of the realities of that risk. For instance if we have identified the scarcity of skills in the meteorological field as a risk, as a key risk, we will then say what are the plans that we should actually generate to mitigate that risk. One day we had a problem that was approved by the board, that we prevented to happen, which is the attraction and retention problem. In it you have a component that looks into skills transfer because we have identified a particular discipline as scarce skills, and we are saying those that have the skills, despite the fact that they may be judged to be scarce, must of necessity and out of the problem, transfer the skills to the less-skilled one, so that we multiply the pool of the skills. And then you also have your attraction program which relates for instance, we never used to structure our salaries and so now when you want to sell the organization you also indicate that one of the things that the organization does is you can structure your package. It does not apply to senior management or executives only; it applies to everyone.

Is it?

For as long as you have a certain compliance and things you take into consideration like your UIF, your pension fund/provident fund – whichever applies – and also we invented a recognition program which was not in existence, we just invented it some four years back, and that means there is an award where we have all the nominated employees from different offices in the country, participating in an award ceremony – that happens only once a year towards the end of the year. And so by that we recognize the performance, we recognize also those people that have gone an

extraordinary mile, to make the point that they are performing within the organization. And so that is how we normally try to generate programs that mitigate.

I think that is well understood. So I just want to make sure, we talked about the risk identification assessment and the mitigation. So we are saying what forms the basis. So all these identified risks and assessments and the mitigation plans will be captured where?

They will be captured in the risk document. There are risk committee meetings, at which those particular risks are discussed and the programs are put into place to say what it is we are doing to mitigate the risk and how far have we gone in terms of implementing those programs. And on a quarterly basis we convene that meeting and that structure is accountable for its management within the organization, but ordinarily the EXCO members, as heads of particular divisions, will then cascade down those risks to divisional plans.

Yes, because that is exactly what I want to understand there, because my understanding of what you are explaining now is at a strategic level, right?

Yes.

Now at the operational level..

Ja, you cascade those organizational risks, those are strategic risks, you cascade down to operational level; even in that operational level you lift them up because they are organizational risk, and then we have a section that talks to operational risk; those are the risks that you normally have to actually manage by virtue of your position in an organization. You understand?

Yes.

So pay roll issues that we need to sign each time we authorize payment of people – all those particular things – relief management, recruitment processes and various other things.

Okay, so at strategic level there will be risks that come from the top there.

Ja, organizational strategic risks.

Yes, and from the operational also, there will also be risks that come directly from the people at operations?

Exactly.

So there might be different types of risks going down, coming up to strategy, there might be some other risks from strategy going down.

Hm.

So now the risk documents that you are talking about will be both at the strategic and at the operational.

Yes.

So at some stage you will then match the two.

Not necessarily match; they complement each other, because I have indicated that there are controls..

Is it two separate documents?

Yes. It would be two separate documents but they complement each other because the divisional risk plans are not necessarily discussed at that strategic level by the committee, but for instance you inform the risk community that these are the plans for the divisions that have been given up, so they have a glimpse of what a particular risk for a division is. But in terms of working on those risks, it is entirely the responsibility of the divisional head and the departmental managers. However, for strategic reasons, the management, coordination and accountability of management of those risks lies with EXCO. For instance if there is a risk that talks to HCM, it is me that will be talking to that risk at that level.

What is HCM?

Implemented HR

Why HCM?

Human capital management.

Okay.

And from that strategic list you will have different risks that pertain to divisions and those divisional heads handle them.

Ja. I get that. So from those divisional risks then, that strategic risk that is sitting there, it does have an idea of what is the issues in the divisions?

Exactly.

So in other words in answering question 1 I would be correct to say that the division will identify and assist in whatever mitigation plans that form the basis of the strategic ones, because the strategic..

Well in part form the basis of the strategic one, in part: you see I don't want entirely they form the basis, I would say in part because for instance the risk that we have identified, the scarcity of the science discipline, it is not…

Divisional.

It is a divisional risk but it is not a challenge that is peculiar to SA; it is a worldwide phenomenon, if you get my point. So as much as you will have your initiatives in that you are attracting and recruiting from the same scarce pool in the country, you will also have to have a leadership of the organization pitching at a higher level, where we are actually collaborating with other organizations outside the country – either for skills upgrade or for secondment of other scientists in the country or for actually looking for positions wherein people can actually go overseas or wherever in the country, to amass certain specific skills you see? But that cannot be an operational function, it is at that level, that is why I am saying in part.

Happiness. I am closing question 1. Question 2: how are the organizational risks integrated and encompassed into the formulation of the strategy or strategic objectives – as well as the operational plans for the organization? So I am asking from you: when you set out the strategic objectives and when you set up the organization plans, because it is going to be at the strategic and operational level, do these objectives and plans get encompassed from this method we spoke about, the risk registers, or not really?

You are saying to what extent is the strategic plan influenced by the risk profile of the organization?

Yes, yes, yes.

Right. That's the answer. In part the strategic plan of the organization is a point where the organization wants to be, and factors that ought to be taken into account in working

out that plan are the particular strategic risks that have been identified in the organization that can hinder the achievement of the targets in that, and how we do that, we then phrase or work out an objective that will be directly responding to that strategic risk identified. Right?

Yes.

So there is a continuum between the strategic risk as well as the plan of the organization; it is a balancing act. Hence in a strategic plan of the organization, dealing with the question of scarcity of the scientific skills in the country, we have an objective that talks to the creation of a strategic reason who will look at capacity for our performance, right, where we are looking at the availability of skills in the organization and the creation of the scientific pool in the atmospheric science discipline.

Okay, but what comes first? So we will go as EXCO, as whatever the top management, and decide this is the strategic objectives for the organization for this coming financial year. So we will set the objectives first and then go and look at the risks.

No, in fact there is a strategic plan that spends… in fact it used to spend for three years, but now it is a five year plan and that plan will be reviewed on a year to year basis, to make it a living document because it has to talk to what is happening in reality to the organization. And so when we also have a strategic risk profile of the organization, that risk profile sort of gives you an understanding of the kind of risk profile of the organization and then when you review the strategy you already have an understanding of what the risk profile is and hence when you review your strategy in terms of the attainment of those objectives you will then work out activities or targets that will seem to what of these risks or alternatively you manage your risks such that they contribute to the objective attainment that is in this strategy. And so helicopter view, you have two documents talking to each other. The other one is the road map to achieve organizational goals and the other one says that this is a red light, these are the things that you should take into account when doing activities towards attainment of that goal. And then this one informs this, or not informs, but the strategic plan must factor in this profile of the organization.

Happy. So that takes care of question 3. Some of them will seem like it is the same thing but I think for academic purposes there is going to be repetition. So again here, I want this now in your own words: how significant…

Those were my own words throughout! (laughter) Unless you are doubting that I am talking from the cuff.

No, no, I want you to just rather stamp this one so that I am very clear: how significant is the role of risk or the whole risk concept when the strategy is being set? This road map we are talking about: when you are setting objectives to say this is where you want to go, I understand that you said there will be that road map and there will be this document that might keep this one in check, but now how important is it that a risk must be… or is it important for you when you do the strategy formulation, to consider the risk? Or can you still do the formulation without?

It will be like separating blood from water, or vice versa. It will be like thinking of blood without an element of being liquid. They talk to each other quite significantly. The strategy of an organization cannot be a workable program without factoring the risk profile of the organization, because the risk profile provides you with signals that you will always have to be aligned to, in the formulation of a strategy as well as the execution of the strategy, because formulation could be a bit easy without a strategy but the test lies in the execution of the strategy and if you don't factor in the risk profile of the organization the hindrances will be encountered when you are executing the strategy. It is like a car without a test, it is a car, but you are not sure if it will reach Durban if you are not joined together.

Okay, I get that. I am just wondering, was it always like that or was it because of the recent governance structures, was it always like this, because I know in other public sector institutions they are not into the risk thing yet. They are still going to come there, because even here I am sure you implemented this risk thing a few years ago?

Ja.

So before that what was happening, it was just risk and objectives and move forward? Or maybe risk was..

There was, but it didn't have prominence. There was, probably its term has changed as well; you will hear people saying 'what are the challenges that the organization have?' And in most other organizations they used to say what are the challenges, what are the bottlenecks you see? But now those challenges and bottlenecks – here is in and here

is out – they have proven to be the key factors that stagnate the achievement of certain targets and objectives, hence it was elevated into being the field of risk management.

I agree, because like I was saying some other public institutions are not there yet, but I am very glad for what you are saying.

It is not a novel phenomenon or discourse, it is there but it wasn't a structured discourse; now it is structured and there is a better insight into what the organization needs to do and people that would be executing that function as well, because it is another issue to identify risk if you can't manage it because you lack capacity to do that; it is a risk on its own.

Ja. Happiness there. Question 4: Does the organization know how much risk it is willing to take? In other words the risk appetite or the risk tolerance? So I want to understand here, what is your organization's policy or policy or maybe unwritten policy?

It varies, it depends on the risk, on the nature of the risk. There are risks you can absorb, you know if for instance somebody said insurance could be costing me say R200 a month, and you look at the number of chairs you have you see, the insuring of the risk may be too valuable a financial obligation to take and maybe we can absorb the risk by not insuring them and making the point that it is fire proof and everything. So it varies from the equipment we insure to actually formulating the risk. There are those that you would actually take the risk and there are those that we will get that party to cover risk for us. You see? Like the asset base of the organization, it is a risk on its own, the information of the organization is a risk and those are the things that we cannot do without having somebody else hedging us against the possibility of that risk.

Okay.

So we don't have a blanket policy.

So it is like a cost benefit analysis. You know how much it costs and what are the benefits, and if they don't warrant…

Ja, cost is not only financial, cost could be that it is costly to lose the information, but in terms of not only financial, but even…

Like qualitative.

Yes, qualititative, because you can't replace them with money if you lose the information, you can't say I have a billion rand and I want information – you won't get it anywhere. And so the replacement value is also important.

I got you. No. 5: is there a point before finalizing the strategy where you can comfortably say that we have covered all the possibilities as far as risk is concerned? Say for instance you are in human capital, I suppose it is a division of its own. Now in this division there will be your objectives for human capital for the next financial year. That will also I guess be informed by the strategic objectives. So when you do your own objectives at the divisional level and at the strategic level, can you get to a point where you will say okay this is the strategy and now we are happy with the strategy that we have considered every possibility of what can go wrong. Or is it not possible?

Well you can't eliminate all risks.

But you can get some comfort.

But you can get to a level of comfort, to say that you have covered enough ground.

Yes, that is what I am asking.

To ensure the sustainability of the organization. The risk discourse itself is about the sustainability of an organization and so once you get to the core of sustaining the organization using the documents you may have generated and what we have put into place, that can give a level of satisfaction that you have covered, in a way you are satisfied that the organization is in good hands.

So the answer is yes we can get to a state where we have sort of covered, though we can't completely eliminate.

Quite.

But we can get to some comfort level to say you know what, …

It is possible, there is that level, but just as I indicate you can't eliminate everything, there will always be further development.

Yes, because things change. Yes.

Yes, an innovative ways to cover even those things that you may have not covered. But there is a level of comfort and it is mainly owing to the fact that on the basis of the

risk that you yourself may have identified in the organization, you will have had management avoiding, and management of those risks you can avoid them, you can transfer the risk to somebody else – and that is the good thing about it.

But from where you are sitting, you feel that at least for now you have covered as far as you understand, the organization has covered its bases?

Well not necessarily because it is a moot point, because you want to get enough resources to get to that level of satisfaction that you have covered the risk.

So there are not enough resources for now.

There is not enough resources to cover risk, in fact it is in the nature of this discourse as well that you may identify certain risks for which you do not have enough resources, you see, meaning that if you don't have enough resources you just manage that risk. You see? In a way that you know it can happen but if it does happen the impact of it is less than when you did not manage it.

Yes. 100%. This is the new one. So we have done 5, we are on no. 6 and all in all there are 12 questions.

You are half way through.

Yes. No. 6: Can the risk profile change after you have said you have formulated the strategy, can it change after formulation and during execution? Because remember you formulate the strategy and you go and execute. So now if during execution you suddenly realize that this is more or lesser than what you expected, what would happen? If you get to realize that now these objectives you can't really…

It can change. The risk profile. The amount of activities that we execute to mitigate or avoid or manage the risk must have an impact in terms of the level of that risk. You see when you first identify the risk it will ordinarily be on a high risk profile, and then as we implement activities, and in controlling that risk or even managing that risk with whatever way you choose to manage your risk, the risk lessens; it is either eliminated completely, or it becomes moderate. Or you even probably, the possibility of it happening, the likelihood if it was 90%, you even manage that component and then it becomes 50%. And so those particular changes that are the function of the execution of certain activities on identified risk, are in themselves enablers in changing the risk profile of the organization.

Okay. So now in that instance you go and re-assess your risks?

Yes.

This was high, not it is moderate.

That is why I am saying as time goes on you assess your risk and then because the risk profile of the organization has to be a living document, and you then say we move from this risk which was high, to moderate – and you adjust it accordingly. For instance for a meeting in … it could have been high and in argus it would have been moderate – depending in the impact of what we have implemented.

And you are saying it is a living document, meaning it is updated all the time?

Not all the time, but the activities are ongoing.

But how often do you update the actual document?

Well it will be once in two months or something.

There is nothing like a monthly update?

It is operational and divisional risk, that you get every month, but as for the strategic risk of the organization you implement the activity and you report the activity and you assess the impact. And then when you are meeting you just look at what you got from the activities.

I am happy with that on strategic level. On operational level how often, do you know?

Well it is done mostly because there will be monthly divisional meetings. And in those monthly meetings as much as we are discussing operational issues, risk is part and parcel of that, in the event that there is an activity that necessitates a change in the risk profile, and so it is a document that is reviewed on a monthly basis by virtue of the monthly meetings that we have in the departments.

Tell me, in this monthly meeting, does risk become an agenda item, or is it just a by the way?

No, it is an agenda item. It is an agenda item. Sometimes it is not title the risk, for instance we are an ISO certified organization. The risk is to lose the status. It means that the human capital division must do its part to ensure that there is a retainment of

that certification – and that is a risk – retention of the ISO accreditation. And then what you will have in the HCM meeting is the topic that talks to total quality management. You see?

Yes.

And by discussing that topic in that meeting you again are attending to a particular risk.

Okay. Question 7: I think you have answered, but let me just make sure again. How often is the review of the organizational strategies performed and aligned to the achievement objectives?

The organizational strategy – not the risk.

Ja. No, remember when you review the strategy, I assumed that meant you were talking about when you review it you will also be looking at the risk one.

Ja, you do that, you look at the risk one as well. You do it on a yearly basis, however in reviewing it, there will be quarterly feedback on progress, it is a compliance issue; it is done quarterly where you look at where you are and the implementation of the activities. It is also at that time where you will be looking at your profile and at your risk and seeing what impact they have on the implementation of your program. So I will say formally it is yearly but on a day-to-day activities of the organization, when we implement a strategy we review it on a quarterly basis, we take account of the risk activities that were emerging.

And that is the point now at a strategic level where you will maybe also update the risk profile at a strategic level?

It informs, it forms the basis of what you cascade to the update of the risk at a strategic level, ja.

Okay, I get that.

Because reviewing it may also mean not changing anything.

Yes.

If there is nothing that necessitates a change.

Yes.

And so it can be reviewing it by way of amending or reviewing it by way of saying the risk profile is still the same.

Yes. No 8: Specifics now: what are the specific steps involved during the review? Can you say in steps that we do this when we do the review, or there isn't anything?

Well we look at the portfolio of evidence in terms of the achievement of milestones. We will have a program and a milestone and in the event there is no milestone it could be probably an activity that is a once off activity. And that informs you to say this is what I will carry through to put in a proper support, because in the risk profile we have a complement that talks to the proper support – as at this date this is what we have done, and the impact that it had on the risk profile of the organization. And then we will then meet as a risk committee and then you indicate these other activities that you have done in addressing a particular thing, in your assessment, this could have been… people will have different views, some will say this is not entirely eliminated and there is a portion of the risk that still remains, for which we have to do certain activities. Because it has to be an objective assessment as well and that is how it comes about but it is structured in the sense that the meeting makes it a structured engagement, but it is not like there is a SOP that says for instance this is how you review the role and it is mechanical.

But shouldn't it be mechanical? Because I think that is a very important activity.

I won't answer with a monosyllabic answer but yes and no, there will be a risk but it may not necessarily need an SOP. But there will be a risk that you will need an SOP to do, depending on the nature of the risk and the level of the risk in terms of the probability of it happening, yes you may need it; because it may be too tedious an activity to have an SOP for each and every risk you have identified in the organization.

I understand, I was just saying for that review that takes place, shouldn't there be an SOP?

There should be.

This must happen, maybe this evidence to be provided by the officer.

For continuous improvement there is that gap; there is room for improvement there.

Okay.

To say we can generate an SOP on reviewing of risk.

Okay. And so that is that.

But maybe there are also SOPS relating to review of documents. But there is nothing specific that pertains to..

..to the strategic level.

…strategic risk of something. Generally when people review things they review it just like it is supposed to be reviewed, like any other document ought to be reviewed.

For whatever portfolio. So I suppose that SOP for review might very well cover the review of the strategy also.

It could.

Okay. What is the significance and evidence of the enterprise risk during the review process? Okay, so here I am trying to find out what evidence is there to show that a review happened and the review took into account the risk profile?

Well it is the strategic document that is a product of that review, because it will be different to the ones…

…before the review.

Ja. That is the only tangible proof that one would have. And also in terms of the risk, strategic risk, ordinarily there would be activities that will have taken place that were not there initially.

So maybe even the risk profile might change during the review because other things might come up?

It can worsen, it can change, and it can go either way because in the process of review you may find a gap that you missed in the previous meeting or previous assessment of the risk.

Or something new.

Or something new that just came up. But that is true.

So if the AGO ever wants evidence of the review it will be the actual document because it could have changed, ne?

Definitely you will find changes. In fact yesterday we were finalizing a strategy document and that piece of document is different from the one we had before.

That makes sense. No. 10: does risk management form part of the KPIs or job profiles?

Yes it does.

For who?

For various positions, particularly at management level. Definitely you have the KPI of that talks to risk.

From management.

Ja, but it is your responsibility then to cascade it to different people.

Because I would imagine it would be everybody's responsibility?

Well it is, but that is why I am saying that in other subordinates it will be an activity that takes care of the management of risk, but is adjudged by that person as part of their daily activity. You see what I mean? But as you go up you can see there is a skewed approach towards identifying that risk specifically. You see?

So in other words, yes, it is everybody's responsibility, it is not really in the lower level KPIs.

It is, but I am saying that the manner in which it is captured, in the lower levels it is captured such that it is engrained in the work, their day to day activities.

It becomes part of the work profile.

Exactly.

Okay. Shouldn't I maybe just ask this, this is what I am thinking now in my head: shouldn't it be clear even from the lowest level that you know, risk management is everybody's responsibility? These activities that you do here, 123, are part of risk management?

It depends on the level of maturity of the organization. And the skills level of the people to whom you want to do that. To a person with some basic post matric qualification yes you can do so, and there could be a level of understanding, but to a cleaner, if you are

saying that he is managing the risk he will ask you why? It is his not his job, his job is to clean the floor.

Understood.

But maybe it depends also on how you coach that management on risk in terms of the lower end of the workers: if for instance you say that if you don't sweep the floor dry there is a possibility that somebody may fall and get injured, then it has a different tone. There is a motivation to clean the floor dry so that doesn't happen. But you don't say to him 'you are managing a risk' (laughter).

I understand that. How exactly does the risk management system, whatever system that is being used, the registers and all of that, how do they affect the allocation of resources in the organization, being human or non-human?

They are set up, particularly there are risks that talk to the sustainability of the organization, it is one key element that we always have to guard against, we mustn't be like any other science institution, we are a peculiar science institute because of the kind of products and services that we give. We are not like for instance a laboratory just like any other laboratory; we have a particular science discipline, so that on its own says that more resources have to be given to operations, so that there is a sustainment of our character as an organization that is a premier national organization. And so operations is where the core staff is, and so in the past, in the slicing of the pie, you basically have to give the larger portion to operations because you are guarding that.

So what is the core… okay the core business would be… maybe say in aviation for instance, the giving of information.

Ja, the core function is to give critical information.

Yes.

You see? But what is more important is the purpose for which that information is issued; so for safety and property.

Yeah, so now the important thing is to give almost accurate information.

Ja, it is to…because the nature of our service is based on probabilities, you know statistics – it is based on probabilities and then you issue information. And time frames do play a major role in actually adjusting the level of confidence. The longer the time

frame the less probability it will happen, but as you get closer to the date, it is more probability and the level of confidence of the person that is issuing, rises.

Yes. So it is now what, the equipment, and the specialists, the experts in your organization?

It is a function of a plenty of things: systems, expertise, infrastructure. The systems, the bandwidth, the dissemination of information, the transmission of information to the nerve centre of the organization, that is where they look at it using expertise, and interpret the data that comes through you see?

Ja, that just boggles my mind, So also the sea…

Yes, marine-focused: And basically for safety of life at sea and also part for preservation of the marine population because it is a source of food. You eat fish, isn't it?

Yes.

Mind you I am not a scientific.

Yes

Okay. Allocation of resources we have done. I think we are on the last question. Please explain to me how the risk management is perceived? Okay yes, on compliance level, now this last question is on the compliance level. Remember as an organization you need to comply with whatever other laws are out there - international and all sorts of things that we comply by. And also, in fact I am not sure of this one, but also you might also have to influence other people to comply by your own laws. So in other words as an organization you comply by the international laws, but some other institutions need to comply by your laws. Are there institutions that need to comply by your laws?

Yes, just like Italy. Italy source their information somewhere else

So this question here is saying in terms of compliance do you think that the risk management processes endeavours in this company have been to comply with those that you need to comply by?

Regulatory – yes, but in terms of other third parties complying with what they are supposed to comply with, there is room for improvement there, by tightening the legislation to be punitive and to have the control platform to do so.

Yes. Okay. So now in terms of this, the risk registers and all that risk profile stuff, does it help your organization comply with international rules.

Yes, it does

But it does not necessarily help your organization to get the regulated parties to comply.

Yes. That is what I am saying. The complying is not external.

I think we have come to the end of the questionnaire and thank you very much.

ENDS.

9.3 2013-08-07 10h00 Interview

So as discussed I am going to start with the questions, and also give you a copy maybe, just to see the questions I am asking. And you are welcome to take your time answering in however way that makes you satisfied.

So I am going to start with the first question, I am going to break it down into three questions, I realized if I answer it in one thing it gets too much. So for the first question: I want to understand what forms the basis of risk identification here at your organization. How would you say 'this is how you identify the risks'? Remember my whole thing here is around strategic risk. So you would have had strategic objectives or the strategy and there will be risks from wherever in the organization – internal risks. So how do you identify those risks that might be a problem to the strategic objectives?

So the process we follow.

Yes, the process, everything – everything involved.

Okay, I am part of the executive so they call us EXCO, so after we have developed a strategy we sit as EXCO members, and we also make use of a service provider so they can channel us.

Service provider?

Ja, a service provider. For example we come with a template of the risks and we look at that template, if we want to adapt it somehow, but what is important as EXCO is we sit, we first want to find out what the high level first risk is, that which we think is very important to elevate. So we discuss those risks. We have different divisions, so I am operations, so I am mostly making sure that I am focusing on operations; it is not that I am not going to talk on other areas, but to make sure that with operations I am coming across as an executive. So once we agree, we debate those risks you know, that have important impacts, and then they are rating it, how we should rate it and then why. So then we prioritize them and give them colour codings. But then after that, in operations I have got six departments – so your division is your EXCO and then the department is headed by senior managers.

So there will be six senior managers.

Six senior managers, that is mostly the core, focused in aviation and related matters, your IT, your Technical services i.e. looking after the network – it is maintenance, all the networks, lightning protection network, observation network. Okay? And then we have got air quality, which is a new mandate that we have just got as an organization, I think about two or three years ago.

Is it new mandate from who?

In the mandate from the Department of Environmental Affairs. We had several mandates related, public services, and then for commercial. But now we have air quality as an additional mandate.

So it is not part of commercial or public?

No it is an additional mandate, it has got its own guidelines but then we didn't want to cloud strategic level, we wanted to come up with high level risk. But then I go back now as operations and I sit with my senior managers, and then we have got this risk, but that risk is informed by various potential risk, you know, at low level. So for example if we would mitigate a risk, what is it that ought to be done. For example, I will give you one of the risks, it is insufficient funding to support the mandates of the organization. But here at operational level there are also some lobbying activities we need to do you know, that assist executives to lobby with the shareholder, with the portfolio committee, with treasury – so that they can understand the need and also the consequences of having this funding not improving from where it is at the moment.

Okay, the same example you are using, the funding, because now I am interested in understanding whether the identified risks would be coming from the top down to staff or would they be coming from the staff, from the bottom, and emerging going up?

It is a top down, but that is the formal process. For example I would have an engaged already, you can see there are various expertise in my division you know, I am more of an expert , but then my IT skills might be limited, depending on my experience. So that means if I don't consult there I might be leaving information. Okay, so that when I go to EXCO I am more aware of how my departments are working, and the managers would also have consulted with the unit managers – some of them you know – depending on the level of understanding of each unit.

So now each unit within operations will have their own identified risks based on that unit's objectives?

Yes, each department. So what we do monthly, we are having our audit, audit and risk is the board; EXCO have a risk committee okay? So those senior managers, we call them department senior managers, I would have shared with them the risk register and then the action plan and it is actually them who assist me to populate, they would populate for their departments, and innovation – if for example there is a new risk that is identified he is going to bring it in, so when I go to EXCO I would like to update the risk register. I think the risk register needs to be elevated.

So now each of the departments will have their own risk register, so based on those departmental risk registers you will then update the high level risk register, the strategic risk register.

Ja, actually the way we are doing it, each division has got a risk register and also an action plan or an implementation plan.

But when you say division, you mean not department division?

EXCO.

EXCO yes. Okay.

Then my operations risk register actually represent the department as well, okay?

Yes.

So this is the operations risk register, these are the risks that are talking to me, but then depending on the details that are coming in there, so when I report to EXCO you know moes, maybe the department may be complaining about petty things, e.g. my department ideally is supposed to have 20 personnel, but I only have17, you know? And then you find the re-alignment process, you say that one is okay with the 17, but you know the people will tell you not to internalize some of the decisions that are made; everybody wants to push for his or her area. So then I am not going to bring up everything.

Yes, yes. Exactly.

But operations risk is the one that is used by all the departments, so they just identify 'well this talks to me'. So you won't find a formal process that forces each department to have its own risk – no. It is operations, they talk to operations.

Okay, but they can still come with their own risks and add to the operations?

Yes.

If maybe in the organization there is something new that comes up as a risk, then they can always add to that, or at IT or something.

Actually operations is also submitted to EXCO and it is much now bigger document compared to the one that is just high level risk; you know, it highlights these are the high levels, but under each of the operations there are those identified that are talking to the high level. So then it expands the document.

I think I get that very clearly thank you. Now on the assessment, those identified risks, you assessed them at what stage?

At EXCO

At EXCO level. You don't include the departments when you do the assessments?

When we do the assessments we assess them at the EXCO level, then each head, like me, then goes back to the departments as part of communicating the outcome of the assessment. So if then my departments feel that no, no, probably you could not articulate this risk, remember the consequences of this – so then I will bring it back to EXCO.

Okay, so they all have some input into that.

They have input and also an acceptance of the document. Because when I accept it as operations, that means they are happy that their inputs have been taken care of.

Okay. This mitigation plans – so in the same document we are talking about there will be risk identification, so there will identified risks, those risks will be assessed with the input from the staff, and the action plans going forward to mitigate these risks will also be in consultation with the same process, with the staff.

Definitely.

So everybody is very aware of what their risks are and how they are being managed and all of that.

Yes.

Okay. So that is no. 1.

But as you are coming in, we have just changed the format which has been now presented to the board – in which month are we now? August. Ja. 20 July, I just don't remember now, but the format is now a new format.

Format of..?

Your risk register, your activation plan.

New format? But who brings the new format?

You know it is the way our service provider comes across.

Who is the service provider?

Who is it, I have forgotten their name.

The auditors? Or not really.

The internal auditors.

Yes. The internal audit is done by… is it not Sizwe?

No, no, it is not Sizwe. You see they are also new, they are fairly new. But you will easily get the name.

Okay. So you are saying that just the template has been updated.

I mean as you speak to different people, I am just making you aware.

Ja, because definitely yesterday the discussions we had, no-one pointed that out.

Ja, because we have just had a board meeting so we still now need to populate it.

The new template.

Ja, it must still go to operations. But it is not really a substantive change, e.g. the other service provider would say 'lack of high performance computing' – you know?

Yes. Because that is the right terminology – 'lack of'

And the other one will change it and say 'lack of', because it is existing but its capacity is not sufficient.

So maybe then say 'insufficient', instead of lack of.

Ja, whereas the previous service provider wanted us to look at the total negative.

Yes. Okay. So no. 1 is done. Some of them will seem the same thing but just for our clarity for our academic purposes we will still have to answer them and just make sure. Also I think for purposes of transcribing, so she is very clear on what the answer is.

Right.

How are the organizational risks integrated and encompassed into the formulation of the strategy or of the strategic objectives, as well as the operational plans for the organization? For question two here, I think the direct link is that remember there will be operational plans, and there will be at a high level the strategic objectives. Ne?

Ja.

So I just want no. 2 to be clear, that when we are talking strategic objectives or when we are talking operational plans, what is the link at both levels to this register that we are talking about – whether that same register talks to both or whether at different levels it gets influenced in different ways?

Okay, the operational plans will be influenced by the strategic objectives. So the risk register becomes one of the documents that we use as we develop a new strategy. Because in the new strategy remember we also identify areas that will need resources, and also where you elevate some of the risk; you cannot elevate all. I will just give you an example of the high performance computing capability needs: as we have presented over the years to treasury, to the department, it was like there are other high performance computing in the country, why can't you use them. Then when we elevated that in our strategy because the high performance computing, the core of this organization relies on it, otherwise you won't have the services when it is down or not capable of performing its duty, so they have innovated it at a strategic level, so then as you come to our operational plans it was already high level. So then that means I could

easily put it in the agenda to the CEO when we have bilateral meetings with her department and a meeting with the minister you know, and the meeting with the portfolio committee. But the most important one is the bilateral with the department, some of them would include invitation of treasury for example. So then it changes the whole understanding now, that all this high performance computing is used differently here and is 24/7 – hence they cannot be able to share with the other organizations. So hence we got the funding for high performance computing. You know? But what I am trying to communicate to you, it came through that it elevated, when it came up with our strategic objectives, and then the awareness to the department, to the bilaterals were being fed from the operational plans.

Okay. So we are saying the operational plans, like you correctly said, are directed by the strategic plans.

Yes.

The strategic plans of which you would have been influenced directly by the risks identified.

Yes. I have just taken one example you know, one that it got elevated, and then the results were positive.

Ja. So now at the operational planning level, they don't necessarily have to go to the risk register, because they would assume that the strategic plans which they use have already taken into consideration. Or can they when they do the operational plans, still also go back.

Yes, yes. Because remember the operational plans also get into details of informing them, mitigation. You might identify it at high level but not clear about the details on the required activities that a certain line manager must action for example. So then the way I put it, it gets serviced from the operations level.

Hm. Okay.

But what is nice now you see, already in the operational level it is known that those are the risks that are supported by EXCO, considered key risks by EXCO, so they must be taken seriously by the organization.

Yes, yes. Okay, I think I am very happy with that. It is clear. For no. 3: how significant, because I am sure we have sort of covered it but I want you to still

say here how you think, what is the significance of the whole risk thing when the strategy is being formulated?

I mean the risk concept for sure is very, very significant. I just gave the example of high performance computing, it was talking to very limited backup and here we are dealing with huge sets of data. You know? And if you mess up with that data, that is the data that also informs the services change for example, it goes to 150 years ago, you know? But that data also needs to be processed.

Every time I listen to this organization's service thing, I just cannot imagine.

So then the risk concept is very serious, and then when you form a strategy you find you have got all the senior managers, all the regional managers and some key unit managers. So it is also an opportunity to emphasize it there.

So for strategy formulation you include all the other managers?

All the senior managers. Normally there is a director or something but… and then definitely all the regional managers – we have five regions – and they have smaller offices under them. So they are automatically part of the strategy. But you have also got unit managers, a couple here in the head office for example, but not all get invited, you know; there are those that have either got key roles or experience that we need, or it is part of career pathing or succession plan you know?

There are five regions? Who are the five regions?

The one with the office that is based here, in KZN, then in Nelspruit.

Mpumalanga, ja?

So also Durban, then the other one is at Bloemfontein, and the other is in Port Elizabeth and the other one is in Cape Town. But we have a demarcation as to what regions they are looking at. You are looking at South Eastern Cape, the Northern Cape, Antartic and the Islands, Marion Islands – so that is a big area. But the one in Port Elizabeth would look at the Eastern Cape. Right. And then the one in Durban would look at KZN. And the one in Nelspruit will look at Mpumalanga and Limpopo and Gauteng, and the one in Bloemfontein will look at the Free State and the North West.

Okay, so they are all covered by those five regions.

Yes, but we think they are key because we are outside there.

But for now are they adequate? Shouldn't every region – North West have its own – each one? Or is it sufficient the way it is now.

That could be nice, because one of our needs is to be more visible to the users, to the communities. Because for example we can provide certain information but there is little understanding you know, when it gets to the people there; and also we work closely with other management service providers, so we need to be more influential to local management services structures –i.e the municipal level, and you know – because our means of further disseminating our information, to make sure there are measures in place when needed. So we need that, but it is because of the resources, more especially financial resources. So we cannot…. But again we use the technology for example to take care of other activities that long time ago they needed only human interventions, but some of the things you can actually function using technology. But to go and talk to the community, you can use media, you cannot have a robot though.

I understand that. but just tell me, just under the senior manager ne, when you talk about senior managers, because there is an executive say for yourself in the operation centre, there are senior managers for the different departments: under the senior managers then there would be managers.

Ja, there will be managers.

And then under the managers there are the teams, or the team leaders and then teams.

Ja, you can still for example, for the scientists, you still have your chief scientists, and where in terms of remuneration they are between the manager and the senior manager you know? You still have specialist scientists and others, but then their performance/work sheets are designed such that they have got more time to deal with the science part of the organization.

Ja. Okay. So we answered no. 3 where you were saying the risk is key, key, key to strategy formulation.

No 4: Does the organization know how much risk it is willing to take? So here I am trying to find out is there an official knowledge or practice, even if it is not written down, of what risk appetite your organization is willing to take – or is there tolerance? Like any executive, would they be able to say : 'okay, at your

organization this is what we think our risk appetite is sitting at' – or just by practice this is what we …. I just want a feel of..

Ja, the risk appetite, I know this terminology we were just talking it in our discussions at the moment, you know you don't have the formal process, I understand you have got a formal process where you know the risk appetite can be identified and defined; we don't have that process. We started our discussion around it as we were trying to service commercial strategy for example, because there is some risk in it, when you deal with the commercial side of the business there is some risk that you need to identify and you will take them knowingly that you know here this is our risk appetite. So like for me, I am not an expert in this area, I understand it because it is part of our discussions, sometimes we do formulate strategies and there is a need for that! But I think the practice you know, we know what risk we will take of course because there is a consultation process.

So that is based on what?

On ad hoc identified area.

Just from business knowledge.

Just from business knowledge. And for example the person in the commercial may be able to share more with you in this regard.

Okay, I am happy with that. No. 5: is there a point before you finalise the strategy, where you can comfortably say that 'you know what, now we have covered all the bases that we could think of'. I just want to understand that, when the executives maybe at that level sit and work on the strategy, however many days or how long it takes – before you finalize to say 'okay the strategy for the next five years or the next three years, this is it and you finalize it – before you finalize it what is the level of confidence? Are you at that stage able to say you know what at this stage we have considered everything that you could think of and we are happy that the risks that are key are covered – or according to you is there no way you can say 'now we are comfortable that the risks are sort of more or less covered?

I don't know what you mean by comfortable but there is a stage where we feel 'alright, we have covered…'

Ja.

.. all the risks, but they are always concerned that the resources might limit us in mitigating those risks, so we need to monitor them very closely and secondly we must identify areas where we need to be more aggressive. For example if we have to lobby for funds, if we need to, you know? So more especially recently, the feeling has always been that the funding is nearly killing us, it is insufficient funding.

So the funding is from treasury?

From treasury, for the department. For example in terms of the core skills, we are really thin and getting thinner. The part of the contributor is that we are also involved in training these people, so we are looking for experts – some of them. So we get them from services providers internationally, and they are coaching our people. Like the New Zealand last year, they just took I think three or four, almost within two months. So that was quite significant for us. UK has taken our key people. So then to be able to retain those people you need some incentives and you need a certain level of remuneration. You know? But some of them they don't really worry about remuneration, the scientists they have been wanting these computing abilities to be enhanced a long time ago. But now they cannot better the innovation because there is this limitation which was related to ICT infrastructure. You have got the data, you have acquired new technology, the network has been increased, but it is a huge amount of data that has been added. You need high computing abilities, you need additional skills now to be able to work with this data. So the scientific people, you will find that if they don't get their supporting tools they need, they get frustrated as well. So there are various contributors to losing people. But even the institutions they don't give us enough pull. With the changing conditions, the municipalities developed infrastructure change units there and then they were still taking people from our organization. So funding is always our major concern as we complete the strategy. You feel you have covered all the risk areas and then there is the funding. And then you also have this commercial mandate: if we can be able to generate more revenue that can assist us somehow, but it is not easy to send services, more especially where they are related where people we use not to pay for.

What happens in those cases, do you just have to keep asking for more funding, until you get..

We just keep on trying to find more ways of communicating the need, communicating the potential risk, communicating the possible impact to the country. You know? - Because we are a national service provider. That is why I give you the example of the high performance computing, because we have been wanting it for the past ten years

or so but we only end of last year got an understanding both from the department and treasury, that this is a need. And then when the super computer we have is actually at the end of its useful life, but we just be persistent and find hope. You don't say 'no, I have done all I could do, I am giving up'. You say 'alright, maybe the way I communicate this is not understood, it is not effective'.

Ja. And then the skilled personnel, you can't also take from those New Zealands and the UKs?

I mean the fact that they can leave the country, so they get significant salaries there, and then it comes back.

So you don't hire people that you take from them? Not really.

We have got for example, late last year, through advertising internationally as well, we just looked at some interest, leaning towards two people.

Oh nice.

But what is important for us is to grow the skills within the country because that is sustainable.

Ja. Okay, no. 6: Can the risk profile change after execution? I think we have also sort of answered this but just for formality purposes again, can the risk profile change after formulation, during execution? Remember you will formulate the strategy and then when you start executing the risk profile changes – I am sure it changes all the time.

Ja, it can change. It can change. For example there was a risk that was pointing to the way we manage our shareholder and so forth, hence we are not getting support to get there the high performance computing, but the working relationship changed as we were pursuing it, and then it changed its profile you know? So it is no longer red now.

Yes. So now when it changes I guess that leads us to question 7: when the risk profile changes then obviously there will have to be a review.

Ja.

Of the whole risk profile and of the strategy itself.

Actually the risk profile we are almost reviewing it on a monthly basis, you know, that is why we have got this risk committee and we should meet monthly unless there is

something that comes up that makes us not to meet. We don't wait for a strategy, because the strategy we review it annually. Because you can imagine you might have over-looked a risk, you know you are going to wait for a strategy, but the impact will be serious.

I am happy to hear that because where I am working ne, although I am studying, but I also do exactly those at my organization, so it is sort of the same things really because it should be reviewed every month.

Hm.

So no. 7: how often is the review of the organizational strategy performed – the strategy is an annual review you said, but that whole risk profile thing is sort of a monthly thing.

Sort of monthly activity/confirmation. At least the activities that have happened since the last meeting, you know?

Yes. And you did say there is a risk committee.

There is a risk committee – at EXCO level.

Okay. No. 8: what are the specific steps involved when you review strategy?

For the review: I am not sure about the steps, but what we do is we look at our annual performance plan and we look at the strategy and then we look as to how far we have implemented the strategy. For example last year we did not really want to review the strategy because we felt that there was still second room for us to amend the strategy, you know, whether it was still relevant. Then we went to look whether the implementation plan is delaying us or do we need to adjust it, so last year we actually reviewed the annual performance plan. With the strategy, we just checked the strategy objectives.

So they were still relevant.

Confirmed them you know, and then we didn't even worry about touching the revision, it was like 'okay, let's concentrate on the implementation' – and then we did that. So this year now we are reviewing the strategy, because we feel that we have implemented the previous strategy. Because we were also thinking you don't review for the sake of reviewing; one of the things that hindered some of the implementation was

some resources that became available at a later stage, the expertise that you wanted to bring in you know?

But now the strategy, is it rolling? What is it? Is it like..

Five year strategy.

So when you review this year, are you reviewing for what period?

2014 through to 2019.

Oh, so you will just see if it is still relevant.

Ja. And then confirm. Remember the strategy, we need to have the buy in of the employees as well. So your senior managers and your managers, you still need to check if that buy in is still there.

All the stakeholders, ne?

Ja, we had to learn when we first became an NTT, because the managers felt that the strategy is not talking to the scientific organization, you know?

Hm. But I must say it is very impressive. I didn't even think that our organization would be this much ahead in terms of risk management.

Is it?

Because it is relatively small when I compare it to SARS say for instance, but the progress that has gone on, because most of the public institutions, I don't know what the problem is, they can't move on this risk management thing, I just find it very interesting.

I think one thing is that we know the core that we are hosting and that it is of national interest. That is why every day there is be something about this organization.

Yes.

But it is very interesting.

Hm. So that is why even, you know we can't plan fully, but we first identify key areas, where we have to have a bcp, test it, and when we have to use it we are relieved that we have got it in place, but now we have spread it throughout the organization.

Ja. We did the specific steps. Okay, so you said there is not really specific steps for reviewing the strategies, but the annual performance plan…

There is a step, the first step is to confirm the recommended strategy, that is why we decided not to review the whole strategy, that is the APP, so for me that is a major step we take. Then when we feel that we have implemented the strategy you know, and also we have not really confirmed the APP, so let's review it, we have implemented it, and part of the purpose is to ensure buy in, you know when you work with people if you don't move together you can rest assured you will feel that it has ….So what is important is to confirm the recommendation level and the buy in.

Okay. So we are happy with no 8. No 9: What is the significance and evidence of the enterprise risk during the review process? So what I am trying to find out is when you do the review process, what will be the evidence that shows that risk was a major part of the review? What would be the evidence that will show that after we did the strategic review we did look at the risk. How will I see that?

I don't know how to answer your question, because after that, after your strategy only do we go back to the risk register itself.

Even during review?

Ja, during the review… the risk we don't deal with them as a strategy only, so after the strategy we go then and identify a day to re-look at the risk register – at the beginning or just before the beginning of each financial year.

So it is not done at the same sort of sitting.

It is not a formal process of closing it out at the strategic level; it is used as input and then after that there will be a session to come up with the risk register for the new financial year that is coming, which will be implemented concurrently with the strategy that has just been reviewed.

Okay, I think I get that. No 10: Does risk management form part of the KPI's or the job profiles – I want to know at what level: is it at any level or at what specific levels do you have the KPI's including the risk?

From the EXCO level, we have just had our discussion as we were closing the financial year, that we actually need to make sure that at all levels, because we have a feeling that as much as it is in the performance agreement work sheets, we need to improve in

sync-ing it. So now it is actually almost at the level, because you get it at EXCO level, senior management level, your unit level. Where you have got your focus that for example that deals with users, piece stakeholders, they are at very junior level. So we make sure that in their worksheet, at the entry level, it is addressed.

Ja, though it might not…. On the actual KPI does it say Risk Management?

No, no, it is an activity.

That is directly linked to managing the risk.

Yes.

So at what level will there be a KPI that talks to general risk management, not at any level?

Ja, we have got our corporate secretary, a person who is also hosting the risk register, (I know the board wanted us to have that and appointed somebody specifically for that, but we don't) – so I can imagine in her performance agreement it will talk directly to the risk, but ours talks to related activities or programs.

Yes. Okay, in relation to risk management.

Hm.

No 11: How exactly does the risk management system affect the allocation of resources, being of human or non-human nature? So when you are looking at resources in the organization – I think you did answer this earlier on somewhere – when the resources, whether people or IT or whatever resources are allocated, is it directed by the risks or not really?

Ja, it is, for example I am busy with a masters system plan, which has identified some skills gap on the ICT that need to be addressed urgently. So the first approach now is just to look, ideally at what resources are needed for this NSP, but what are the urgent matters that need to be addressed, and one of them is to have the operations manager with certain skills at the level lower than the senior manager – but with certain skills, because we need those skills. So we look at our audit findings as well, (which had some yellow faces in ICT), and look at the recommendation of the master system that we have just developed. So then in terms of the cost we are too high; they said when we get to the 59%, you know… So then the second action now is to look at the corporations as a whole, so what area that is of less priority that I can use to get funds

to fund that, because that poses a risk for the ICT, and then if in operations I don't get, then I go out and look at the whole organization with my other EXCO members, you know, where can we sacrifice for that so we can get money to fund this post; it is a new post but it is needed. So I have not even gone to the CEO and the general manager human capital – I am talking about the action in progress. So that is how we… because resources will be minimal, what is important is to re-prioritize.

Ja. Okay. I think we are on the last question now: Please explain to me how the risk management is perceived or confirmed by the organization to improve on compliance level by both the organization itself to the laws… let me just explain this.

I think I understand.

You understand? Because I want if possible you to give me a feel of both sides. Say this is your organization in the middle, so I would imagine this organization needs to comply by certain rules or whatever.

International and national

Yes, and over and above your organization having to comply to all sorts of rules, I also am just imagining, I don't know if I am wrong or right, that this organization also has rules that it wants other people, like it creates rules, that some of its stakeholders or customers or whoever, must abide by. So itself abides to rules, and itself also creates rules for other people. So I want to understand how the whole practice or methodology or processes of risk management influence that process of complying to the rules and…

That is the strategic objective: it has informed a compliance, there are strategic objectives that talk to compliance. It talks both nationally and internationally. And then the compliance is also reflected in the risk register itself, in terms of audit findings. But there are so many compliances that we need to adhere to, but there is also another key one that is related to aviation.

Yes.

Okay?

Hm.

So beside the audit we get, there is also an NCAYO audit that we are subjected to, a competency compliance is needed for aviation. Okay? So that is why we actually went to a total quality management system, but for the organization it is not a compliance thing, but for aviation the quality management system is a compliance – not necessarily quality management part, but a quality management system. So one of the few countries that manage to beat a deadline to comply. So those things of quality management systems, your audit, your compliance with related framework, you see them in our risk register and then hence we decided to alleviate that: 'you know what, compliance needs to be reflected in our strategic objective, because it is the risk that can impact significantly'. And also the shareholder, in terms of the BFMA's, because when we approve processes as an NTT, so the non-compliance can have a negative impact; it is easy for executives to lose their jobs with non-compliance.

Hm, with the rules that your organization needs to abide by.

Hm.

And then with the other side? Doesn't this organization also create rules for some other?

We create some rules, we develop policies, like Xanu have their IP policy, so data policy, other people who should use our services – so we do create some...

So where do they get information from?

From global models. So they don't have human intervention. They have models that are generating the information so you can just plug in and they will give out that information – but whether it is accurate or not, It tends to be tested.

So those part of risks are not part of your risk register, the fact that certain entity might not be abiding by the rules – or it is not a risk that…

No, no, it is! We have got a risk on competition, that talks to competition, because we have got many people providing this information and the ordinary people think it is coming from us.

Yes, because sometimes I also just get into my phone for such information or whatever.

Yes, and then there are some misleading emails, I think years back people were misled and had to leave their work places, and they closed, and cars were just all over the

place. And so they looked at those things and said no, that is the risk, we have a related risk.

Okay, you will just sign for me, I think we are done with the interview.

ENDS

9.4 2013-08-08-08h00 Interview

So like I explained, it is a semi-structured interview, so I have structured questions but you will come to answer it any way that makes you comfortable. So you can answer the questions from whatever angle you want to, because the questions are just sort of an indication of the type of information that I want – all in all, however way you want to describe it, it is really okay by me.

So these are the questions, I am going to start on question 1, but because it is a longish question I am going to break it down into three sections, so that you are able to see what I am trying to say here.

Okay.

So the first one here is I want to understand from you, what forms the basis of risk identification, here at your organization? What is the basis that you guys are able to say 'okay, this is how we identify the risks?' Remember that the risks we are talking about are risks to your strategic objectives.

Yes

Because this organization will have its strategy and then the strategic objectives, so whatever you are doing here will somehow be linked to the bigger objectives of the company, or maybe the objectives of your section or department, because those will also cascade into the organizational objectives. So I want to understand how you identify the risks?

Okay. For the whole organization?

Ja, or for your department or division.

Ja, I can say for the whole organization, best we start looking at the sites and facilities, then we look at the staff, the ACT facilities, and then the policies and the procedures, and then we formulate the risk based on those sub-topics. If I may start with the staff: we look at the morale of the staff, the retention of the staff, the skills we have, the training – overall are the staff happy or not happy – and then do we have a risk concerning the staff, whether it be they are leaving the organization, whether the morale is high, whether they will be able to do the work according to the agreement.

Then if we look at the sites and facilities for the organization, we look at the overall sites, looking at maybe if there is a fire here, is everyone protected, what are the plans,

do we have plans in place? Looking at the safety of the staff within the organization, that is when we look at the sites and facilities.

And then if there are policies and procedures in place, whether the policies are implementable, whether they are working or effective, whether the organization does communicate the policies and procedures to the staff. That is what forms the basis, and that is when we start doing the risk, based on all those topics.

So you were saying it is the people, the sites..

… the policies, procedure, ICT facilities, infrastructure and safety.

Okay. So those will form the basis of how they identify the risks.

Yes.

But then those identified risks, where will they be? Where do you capture them?

We capture them at strategic level as well as operational level, and also on our basic plan. So on the strategic level it is a very high level, but on the operations that is where you will break down in detail, that on the basic contingency plan, that is where we have all the risks in detail.

So that is the identification.

Yes.

So I also want to understand after you identify those risks, in the way you have explained the assessment, how do you assess those risks? In other words, say we have ten risks, how do you prioritize to assess them – like this is major, this we can deal with?

We categorize them according to whether they will cripple the organization or not, whether they are more frequent. And then we have others which are red, others which are orange, yellow and green. The ones which are red are the ones that are more critical and more frequent, and the orange ones are the major ones. So we categorize them according to… we colour code them. And then when we review the risk, let's stay strategically which is management, and then operations also review the risk and then do an assessment according to those colours – that is why we categorize them – and then mainly those which are red we prioritize those ones.

The red ones.

Yes.

So now the colours, how do we describe those colours? Is there a specific science behind the colouring, maybe to say from this point on it is red, until this point it is..

Ja, I will talk from the experience what we are doing currently because the strategy is done mostly by the executives. On the BCP ones, the red ones are the ones we categorise according to the budget. So let's say the risk, if it happens, might cost the organization a certain amount of money, e.g. more than R100000 or so, it will be red. So it is according to budget.

I see, so that is how you assess. Okay. And the mitigation plans? Because remember there will be the identified risks, then you will assess them to say this one is red or…

Yes.

Ja, and then the plans to deal with the risks?

Ja, the strategic one, there is a strategic risk management committee looking at the plans, how to mitigate those ones and then operational ones, every division has an individual who is assigned to look at those risks, and then you also have the business contingency plan for the whole organization – those risks identified – then we have mitigation plans also for the ECP for the organization also.

Okay, so now we have covered how you identify the risks and the assessment and then the mitigation plans you saying there are specific people in departments.

Yes.

That will deal with those risks. So every risk will have its own risk manager.

Yes, exactly.

And that person must just follow up to make sure that…

Normally it is the senior manager of each department.

Okay, so they must just make sure that the action plans are implemented.

Exactly. And then also each department has its own retention plans, so it means others which are more critical, like operational which is the core of the organization, they are testing quarterly to check if this happens then what will happen. So they do testing, and then the others which are just supporting they do annually – the testing of those plans.

I am happy with no. 1.

No. 2: Some might seem like the same thing but I think just for academic purposes I want them to be clear, clear. So how are the organizational risks integrated and encompassed into when you formulate the strategy or when you formulate the strategy objectives – as well as the operational plans? So what I am asking is remember there are operational plans, or let me start at the top: there are strategic objectives, and then strategy as to how those objectives are, and then based on those strategic objectives and the strategy from the top, then there is also at operational level the operational plans. So I want to understand when the strategy as far as you understand is formulated from the top, even you guys, or at whatever level, when you do your operational plans, how much do you take into consideration this whole risk, these identified risks from no. 1?

When the organization develops the strategic objectives, they do take the risk into consideration, because if you look at our five objectives, it is mainly also informed by the strategic risk. E.g. the risk which deals with the financial sustainability, there are objectives – and there is a risk which is more on lack of funding, so we are trying to mitigate that risk by having the strategy objective. So most of the objectives we do look at the risk first, before development of the objectives, looking whether we will be able to mitigate that certain risk. So the objective main aim is more to mitigate the risks.

But aren't the risks supposed to be based on the objectives? So it should be objectives first and then the risks? Because these are risks to objectives. Or do we look at the risks first and then create objectives based on the risks?

We do create objectives but also bearing in mind the risk.

Yes.

So we do take into account the risk when we do the objectives, because if I look at all the objectives, and then they are also linked more to the risk.

Okay, so for no. 2 I am saying the risks, the objectives are informed by the risks.

Yes. No exactly informed, but when they develop the objectives we do have a look at the risk.

Yes, maybe we must then say that when the objectives are being developed they take into account what the risks are.

Exactly. Exactly.

So no. 2 I am happy also. No 3: How significant is the role of risk, or the whole risk concept when strategy is being formulated? This one I want clearly to say what do you think is the significance of the whole thing of identifying risks and assessing them in the action plans? How significant or big a part of strategy do you consider, when doing strategy?

When strategy is formulated?

Ja, when you do the strategy and those strategic objectives – whether at strategy level or operational level, because remember at operational we also have operational plans.

Hm.

So when we do those plans, do you completely look at the risks or do you your plans based on what business should be and then consider the risks afterwards?

We do look at the risk but not in detail, especially when we are doing operational plans. We mainly look at the risk on the weaknesses of the organization, when we do the SWOT analysis and that is where the risk comes in. But mainly when formulating strategy, operational strategy, we don't look at the risk in detail. There is another session when we review the risk, which is completely separate.

Ja.

But strategy formulation we only look at part of the risk when we are doing mainly most of the SWOT analysis and the weaknesses of the organization – that is where the risk comes into place there.

Okay, so there is a strategy that is formulated and then there is also a separate section that focuses now to see what the risks are and what is going on.

Exactly.

Okay. No. 4: Does the organization know how much risk it is willing to take? This is the risk appetite or risk tolerance. So how will you explain this organization's risk appetite or tolerance, and to what extent would you say they are prepared to take risks and just tell me what you base that on.

Ja, according to my understanding, we will take a risk exactly as it is. If the risk is a minor and is real then the organization will live with that risk, if it happens, because it is a minor. So my understanding is on the risk register we will tolerate it. But if the risk is major or critical and frequently that is when the organization will say no, we have to look at this risk and how to mitigate it. But if it is minor and rare we can tolerate this risk.

So in other words what is the tolerance level? They do tolerate a lot of risk or not really?

They do tolerate a lot, especially those minor and rare, e.g. if let's say the… if I can make an example of the ICT, the back up, because normally they do back up on Mondays (I am just making an example) and I think three times a week, for example. But if someone comes to do a back up on an every day basis sometimes that is costly and then it might not cripple the organization but if we do a back up on Monday and then we skip another day and so on, then we can live with that. So although there is a risk that the following day you might find some issues but that would be rare, so I think we can live with that risk of not back upping every day but on certain days.

Okay. So you say there is huge appetite for risk?

There is, especially those minor and rare ones. Ja. On operational level. Yes.

And at the strategic, you think it is the same?

No, strategic I don't think they are mainly tolerance; they mainly tolerate those that are beyond the organizational control. E.g. the funding we get from the treasury, from the government, so that is beyond our control, so that we can tolerate and try another means of how to mitigate it.

Okay. No 5: Is there a point before finalizing the strategy or your operational plans, where you can say at this stage I think you know we are comfortable that we have covered all the bases as far as risk is concerned? I want to know when you formulate your plans, maybe the ops plans, and then you also take into account what risks are there and you make your plans trying to mitigate these

risks also. When you have done the plans is it possible you get to a point where you say you know what, according to these plans we are okay, we have covered all the possible things that we could think of. Or do you think that is not possible, to say this time we have covered all the bases at least for now, because you know risk changes all the time, but at that time based on the information you have, can you say okay now we have covered?

No, I don't think so, I don't think we can cover everything in one session. So normally when we do strategy or review of risk we do prioritize but we don't cover almost everything in detail. So I think maybe it is a time factor, there is a time factor, because normally when we have a strategy session it is normally about two days or so and operational risk is normally about one day so you cannot cover everything in one day. So I don't think we cover everything in detail, because a long time ago there was somebody doing the risk for the organization and they covered everything in detail, from the executive stuff, everything – it was more detailed, detailed. But for us we cannot do that because we have other duties, that is why I say when we have a risk review or whatever, we normally look at those important things but we don't cover everything in detail. To be honest.

Okay. I understand. No. 6: I think we have covered this one, but just for the process, can the risk profile change after formulation during execution and what would happen? So for instance now when you were setting up the strategy, the operational plans, this was the risk profile that you had – which means at that stage this is all the risks you thought were important. So that was when you did the plan. So now during execution of the plan things change and the risk profile becomes something else. Those risks that were important are no longer important or vice versa. Maybe there was those that were less important have become more important during the execution of the plan. What happens in that instance, do you go and look at that to see where the profile has changed or maybe not really?

Not really. We only look at risk when we are reviewing the risk, during the review of the strategy or the risk. But it does happen, most of the cases, maybe you find that we didn't find there is a risk here, the security is not effective say for example, and then if maybe the safety manager beefs up the security. There is now a change from being critical and frequent and it changes to minor. So it does happen, especially during implementation of the mitigation plans, things change.

So now when the risk changes we do what?

It is the responsibility of the risk owner to normally update his / her risk register. So when the risk changes it is normally updated.

And then the plans, do they also change?

Yes, the plans do change. E.g. the mitigation plan is to implement, and that thing has been implemented, then it has to change.

Okay. So the risk profile can change. No. 7: How often can / or is the review of the organizational strategy performed? So that plan you have made, whether strategic or operational, how often do you review that plan to align with the risks?

The high level strategy normally is reviewed annually, but operational strategy, we also do it annually but we also look at it on a day to day basis – whether this is still in line. But in terms of whether it is a change according to the risk, is the risk where normally the old risk owner normally has a look at it on a regular basis. And then if he must change the operational thing then it is to conduct especially the GM ops, these things change and now I think maybe the operational has to change. But operation plan normally we do meet no a quarterly basis – as a division – on a quarterly basis, looking at your plan and whether it is still in line - and then also looking at the risk. This is per department now, but the strategy for the organization is being reviewed at this stage on an annual basis.

Okay, so the strategy is annual and the operational plans you say its…

It depends on the department but mostly it is on a quarterly basis.

Quarterly. Okay. No 8: I am sure you can tell me, what are the specifics that are involved during the review of a strategy, or what are the steps when you review strategy or when you review your operational plans? Are there specific steps or is it something that just happens?

No, I think there are steps, ja, there are steps. Because we look at the purpose, whether it is still relevant and then we look at the scope and the vision, the mission. So we look at those steps and then the strategy objectives and then the key indicators, activities. So we look at those steps but you use a certain business model to do those strategy and the OR plan.

So is there a document somewhere or is it just business practice, but not documented?

It is a business practice, I don't think it is documented anywhere that these are the steps you perform.

When you do a review.

But normally there is a certain business model you follow.

Is that business model documented somewhere?

Ja, it depends, because previously we were using sort of a facilitator who comes with a business model saying this and this and this. So we will follow that business model.

Okay. I am happy with no. 9. This one also, I just want to ask this separately, just so I am clear: what is the significance or the evidence that the review process has been done. Like if I say to you, if you say to me last quarter or last month we had a review, what will be the evidence, if I say I come an audit to say that you have done the review, let's see. What will be the evidence to show that the review has been done?

Okay. First you have a session, strategic or an OR plan review and then we review that one, and the first evidence will be the register and the minutes and then after that, after the plan or strategy has been finalized, then it will be presented to the EXCO as well as to the board – that is when it gets approved by the board, and then the evidence is signed off by the board.

That the review happened.

Yes.

Okay, so that one is clear also. So we are on no. 10. Does risk management form part of any key performance indicators or job profiles at any level in the organization? So I want to know from the very low level to the highest level are there levels in the organization who those people's KPI's include other things, but among other things there is a clear risk management component?

I am not sure, high up, but operationally, especially the risk owner, there is that on the agreement, the performance agreement one of the targets must be the review of the

risk and also on those responsible for BCP, it is also on their agreement that it is part of your performance.

But at the lower level it will be the people who are risk owners?

Yes, risk owners, yes. But high level I am not sure, because I am not sure on what their agreement is based on.

Okay, so when you talk about low level, until what level are we saying?

Until the managers level. I think the executives, senior managers and the managers.

So the managers have…

The managers are risk owners and there are also senior risk managers who are also risk owners, but executive wise I am not sure.

And then below managers, there is no one with a KPI that will accept the risk assessment, um risk management?

No, no – that one I think there is no-one. I think there is no-one there. It is from managers.

Alright. So it is from managers.

Ja, and higher up.

Okay, how exactly does the risk management system affect the allocation of resources, being of human or non-human nature? So the human nature one, I want to understand that this risk management system that you have, you know there will be the risk register and then you review it and that, how does that process affect the way you allocate your resources – which is maybe your people, equipment, IT, finances, whatever resources? Do you look into the risk things when you are looking at allocation or not really?

Ja, we do, especially the…. You want non-human first, or just human?

Any one.

Especially the human, when you look at the risk in terms of the staff, we do look at how many people need to be allocated a specific office or specific region or a specific department, and then we will look at how do we normally retain, especially the skilled people, because one of the risks is the retention of the skills, the scientific people. So

we do look at that and then try to allocate some resources in terms of retention of those highly skilled people. So those are the resources are allocated in terms of maintaining the skilled people in the organization. Non-human, there are some areas where it requires non-human resources or simple finance in terms of the infrastructure, allocating it in such a way that it might cause a risk for the organization. And then we also do … it does also affect resources in some areas, for example there was one of the offices which are outside this building where there was a lot of battling, there was a lot of stealing of computers, so we had to allocate resources in terms of..

Is it in the building?

Yes, but it was at Irene, so we had to look at resources in terms of putting a fence there. So it does affect allocation of resources.

Hm, the risk.

Yes.

Okay, the last one: Explain to me how the risk management is perceived or confirmed by the organization to improve on compliance levels, by both the organization itself to the lowest base institution operate within, and to the parties external to the organization which are served by it. So what I am trying to ask is you know this organization on its own as an entity is bound by other laws that it needs to comply to, the operational standards or whatever other laws that SAWS complies with. At the same time, this organization I assume, might also create some rules or laws that it wants other people that it is servicing, to abide by.

Ja.

So it is going to be like this organization is also supposed to abide by the rules, but also makes the rules for whoever they service, your clients, to adhere to some rules. So the risk management processes that you have, how do they help the organization on both sides, to comply to the rules it must comply to and to make sure that the people who are supposed to abide by the rules that you have put in place, also abides?

Ja, I will make an example on aviation because I mainly deal on aviation. There are some rules, called standards or recognitions set by the international body, and our organization has to abide to those standards. And those standards not only affect us, they also affect the airport or airport management. So what the company is doing is in

order for us to get these best products based on your instruments at the airport we have to abide by these rules. And then inform them about the rules. And then what you do also to manage that risk that has not happened, we do have a section where they do an audit.

On..

On.

To see if you are complying with international standards.

Exactly, yes. With the authorities, so they check whether they are accurate, whether they are according to the standards, the requisitions, whether they are giving the right information. So we do have standards, but we do also implement the standards to other stakeholders, whatever it is – that is how we manage that kind of risk in the organization.

But I also want to see a link, if there is, between say the risk registers, you do your risk management system, does that affect the way that your compliance levels, the way you have to comply to international bodies or requirements? Or is that done by this audit division? Or is the risk register helping you to be more compliant?

Ja, on the risk register, that is one of the mitigation plan that we will go there and audit those people, but at some stage, it might happen there is maybe one airport that doesn't want to cooperate, and then it drags down the organization in terms of overall compliance. But we are trying to mitigate by doing an audit on them. So then we also do follow ups so that if there are any issues they do…

So the audit you were saying, was it also one of those to see that you were compliant with the…

No, that was an internal audit, done by the organization, so I was not part of the audit but there were some issues that were involved, there was a need for some clarity there.

So there is an internal audit.

Yes, an internal audit, ja, also auditing internally….

Okay.

There is one question you asked me, about the risk at the managers' level. Below that, it does, but it is not specifically that it is risk.

It is not clear, but they are there.

Exactly, it is part of mitigating the risk, which is part of BCP, it is not clear clear, it is just that you have to do risk management.

I understand that. I think we are done. Thank you very much.

I thought it should be an hour!

Yes, it is an hour. It is an hour, what time did we start? We started just after 8.30. So it is almost ten minutes before an hour. I want to stop now.

ENDS.

9.5 2013-08008-10h00 Interview

I know you are very familiar with the whole risk methodology, but don't give me the answers I want to hear, tell me what you think is the actual situation on the ground.

Not the answers that you want to hear? I am not following completely.

I am trying to say especially because academically you are very familiar with the subject, so I am just saying maybe sometimes you can give me an answer that you think will be the right answer, but there is no right or wrong answer, just the way things are done here in your organization.

No, but you ask me questions and my responses will be as I understand with where we are; I haven't seen the questions but it depends on what the questions are. Because if the questions are generic about one's understanding of the subject matter it is a different story, the level of understanding from different people will not be the same, but if we are talking our organization-specific in terms of where we are, the answers can only be based on the facts because it is going to be based on where we are.

Ja. I fully understand. So the first question, I am going to break it down into three, so that it doesn't become too much. I am going to start with the first part of the first question: what forms the basis of risk identification within your organization? So in your understanding, what is the basis for identifying the risks, when risks are being identified what is it based on?

You can only base the risk identification from your mandate because that is why you want to manage the risks in the first instance, is for you to be able to manage your business or your operations properly so that the risk element is minimal; where you can avoid it, it can be avoided and where you can't then they need to come up with mitigation strategies so that you can minimize the risk. You minimize the exposure of the organization to adverse effects, but holistically what you will base that on is what you seek to achieve, what is your mandate, what are you expected to do and in the process of doing what you have to do then what do you need to do, what is likely to affect your achievement of your mandate in the first instance, then the environment in which you operate – the political, the economic, and all that might affect that. So in the process of doing that then you need to come up with the things, or identify the things that might affect your business and then come up with corrective measures.

Okay. Yes, because that was like what forms the basis of the risk identification. So also in the same one, again, and then the assessment of the risks also – when you assess the high risks and medium and low ones, also what is that based on?

I suppose you said you need to break that sentence down. Those things are inter-related, those elements, because I have explained the first part on the identification element, but do you identify those risks before you get to the assessment and mitigation? Obviously you identify those and you use the risk, once you have come up with the risk and the mitigation elements or plans, then you incorporate that into your organizational strategy because the risks themselves need to be incorporated in your overall organizational strategy, for you to say this is what you intend to achieve, these are your targets and this could hamper your attainment of your targets, and for you to minimize the negative effect of those risks where you can say you cannot avoid them; because others you can avoid, you can come up with the corrective measures that will lead to the complete elimination of these, or you can come up with those that will only minimize the risk. That is where you get to the element of having to agree on the risk appetite, to say with these certain particular elements this has to be done, it is risky but it still has to be done, but as we go along doing it the least we can do is agree that the risk we are willing to take can be limited to a particular threshold and that is where you come up with the risk appetite element. So once you have identified the risks you use them, they inform your strategy, your business plan, so that they become part of your day to day operations. But once you have done that, the assessment and the mitigation plans, you can't just identify risk and sit and do nothing. Once you identify them, then you need to come up with the plans. But once you have done that then if you go through the assessment, the review or assessment – whatever you call it – then you come up with the plans, but on a regular basis you need to review those on an ongoing basis to see if whatever you are doing works, because after identification you come up with some measures to say in order to minimize this one you will do a, b, c, d. But as you go along throughout because of the financial year, you need to go back and say is this working, have we implemented those corrective measures, and if we have can we say that that risk has been reduced as we hoped the corrective measure would minimize the risk or do we need to review. That is why you need to… you can do the annual review once a year but on an ongoing basis you still have to review to see if the corrective measures are actually working.

Okay, as you said it is one question, I just realized that for other people it was easier to break it down and say identification and then assessment, but

obviously you could answer it all in one, so it is fine, I am happy with that. Question 2: Remember some of the questions will look like the same thing but just for my academic purposes I need to still ….So question 2 which you also might have touched on, we were saying how are the organizational risks… remember you were saying you had identified them and assessed them and got your mitigation plans. So I assume that this first step on question 1, the identification and assessment and identification as there will be maybe a system or somewhere where you will have that information or a register?

Yeah.

So you would have them somewhere. Now here I am asking how are those risks as identified and assessed and everything, encompassed into the formulation of the strategy objectives?

I think in a way I have answered that because, ja I have answered that in a way because like I said, you have identified, you have come up with the top ten, top twelve or whatever strategic risks, and in the process of formulating your organizational strategy now, you are taking those into effect, to say okay this is what we want to do but what can stop us from doing that – we have identified these risks, with or without those risks some of the things we still need to go ahead and do because it is part of our mandate; we are expected for example, one particular example from our perspective, we are expected to provide information to our clients, and for us to come up with that advise, the information we give them for operational purposes costs us the some amount of time and energy and they are supposed to pay us for the information provided. But you sometimes get to instances where some clients say they were not part of the original agreement and cannot pay us for that service, but do you then need to take a step back and say do you then not provide the information to that particular one? They are still going to get it, you have a choice to say whether you provide it or not. If you don't provide it you are putting the rest of the public at risk, because if they engage the services of that one service provider who does not have the correct information then and an incident occurs, then the people will say 'but didn't our organization provide the information?' So you are still going to sort of be forced to do that although you are doing that at a loss. So those are all the things, that is the risk you would have identified up front, you know that it costs you and the airline industry is not coming to the party, so maybe when you review the tariffs on an annual basis it is not every year when you agree on the increase you wanted, but you base that increase

on what it costs you to provide the service. But if they don't come to the party then you are operating on a loss, as you formulate your strategy you know that you still have to pay that, you know it is almost going to be at a loss to you because you are not going to be able to recover this amount. Then how do you play around that? It is a risk you have identified but we are still forced to provide the service. The least we can do there is to say this we will do but the effect of it is that it is going to increase your operational costs, the expenses are going to go up but it is not going to match the expenses because you are still going to provide the services and not everybody is paying you. So as you formulate your strategy you need to show that in your strategy for arguments sake, so that when you draw maybe your targets, your commercial revenue targets, you need to show the risks and how you capture that in the strategy then it will reflect that those are some of the elements that will prevent you from reaching your targets but you still have to provide the service and you still have to include that element in your strategy because maybe it is from a public mandate and so you are forced to provide the information, although at times you do it at a loss. So somebody who does the finances at the end of the financial year should understand the strategy, you should tell them up front that you anticipated that and you disclose the risk, you capture the risk in the strategy document as well.

Happiness. No. 3: I want the significance, I just want to clarify, to say as far as you understand, the whole risk concept, the whole risk methodology that your organizattion is using is key to strategy formulation, or there is a risk system that is there, there would be strategy sessions, but there may be the risk is not clear at the time of the strategy sessions.

It has never not been part of the strategy formulation.

So it is a big part.

It can't not be, go to any copy of our organization strategy documents, there won't be a single one that hasn't captured the risk, because even the timing of how we go about doing that, we do the enterprise risk management review in the first quarter of the financial year and we do the strategy in the second quarter or by the time we go to the strategy we have already identified the strategic risk, so there is no way you can leave those out at all.

Okay. Question 4 you have also touched on, the risk appetite and the risk tolerance, but specifically for your organization, do you think that as an

organization it is known, at least to all the people that are involved in the risk system, do they understand and know what your organization's risk appetite is?

Previously I wouldn't say everybody knew what the risk appetite is, and maybe even as management we would go through the enterprise risk management processes and we identify the top ten risks and we know that as part of the risk management processes the board needs to actually agree or approve or set the risk appetite. They need to be agreeable on what we can say we accept, we can deal with this, we can tolerate this. But previously that has not always come out clear and this year for the first time I think we are very clear on that, maybe because the system that we used for the enterprise risk management review and the process facilitated by a different set of people from the ones that have always facilitated our risk assessment review in the past; because this year we said as management around the system we use, we use very transparent, actually I fell in love with the system that the external auditors assisted us with and by the time we walked out of that session as management, we had almost sort of agreed that this one we can leave with this one, but that still has to be taken to the board level once we have come up with that risk register, our risk management report and register already had indications of what our levels of tolerance are, our risk appetite is. So from this year going forward I think we will follow the similar suit as we did with the system; there is some software in the system and ja, I think the risk review process was facilitated but facilitated by our current auditors. We used to use previous auditors but they were using a slightly different approach and this year we walked out that day with risk tolerance levels and appetite having been made clear at management level and then we took that via the audit committee and it was signed off by the board.

So now tell me, is there a system that is used in the organization or was the system the software..

That is the one for the auditors.

Yes, so it was their system so you gave input in the information through. So they work on their system.

Yes, but it was like a live thing because with other things it is not even a question of us agreeing with the other person saying 'I think…' or on some of the elements we literally had to use remote controls to vote and … which is…

Ja, do you know what that system is?

I don't know off my head, it is the internal auditor's system, it is not our organization, it is not the system that we can buy and clear, unless we way in future maybe we want to do it ourselves without having someone from external facilitating. But having sampled it from this side, it makes the whole thing more objective, because in some instances they are able to probe.

Maybe it is still manageable that way, because I am thinking also from where I am working, because it is much bigger, when we do some other things yes there is a system that we will need people remotely, maybe managers from wherever to agree on that same thing like you are saying. Then we all agree to say this is a low risk, this is a high risk – based on everybody's input – but ja, I agree, this makes it much easier. So on this risk question, or maybe before I move to question five on the risk appetite, an official document – so not yet – that explains what this organization's risk appetite is?

Why would there be a single, separate document other than the risk register and the risk report? Because you review your risks on an annual basis.

I am talking about that document that explains what your organization is like…. in other institutions, like for where I am working say, there is a document; you know the risk register is the tools that you use, I understand that, but there is moes a risk policy and strategy and then..

But surely it doesn't deal with the risk appetite

Yes, that is why I am saying there will be the policy, there will be that strategy document, there will be other documents. With those documents there will also be documents that explain what the company's risk appetite is and how you get to it and things like that. So there isn't that document? Not yet?

We don't have a standalone document on their risk appetite, unless you are referring to the Materiality and Significance Framework, but that is not a risk document, it is an overall document for the organization to say it is more finance.

It is a materiality, ja.

That we have, but we don't have a standalone document called Risk Appetite.

It doesn't have to be standalone, it can be a page in your risk methodology or your strategy, that will just specifically though, that page will say 'as far as your

organization is concerned, this is how much risk appetite, as per maybe agreed at a strategic level or operational level'.

You can do that but if you do that, that would only apply for third party, financially, because your circumstances change, your business change.

You can review..

What you consider to be a risk this year might not be a risk next year, because maybe the reason why it was a risk was because you were facing funding constraints, and the following year you get a more reasonable adjustment of the government grant for instance, so you can't have a stated one to say 'this is our…'

No, it is a strategy document, it is not speaking to any one specific risk that will change next year. Like if finance says in your case; this document doesn't talk to the one risk, it is a strategy document so it will just explain at the high level – even at operational level it can explain.

What are you basing that on, from the public service perspective, what provider or the PMFA or the treasury says they must do that standalone document?

It is not a standalone document, in between the risk policies and the risk strategy documents, the risk frameworks – remember it is different documents – so in one of those documents, as you explained how the organization deals with the risk and what they decided to take on as a strategy in as far as risk is concerned ..

And you say it has to be elsewhere other than the risk management report and the risk register?

No, it is not the report, it is not the register: it is part of the strategic document, the frameworks.

I am lost, maybe I am not quite understanding what it is. I understand what you are saying but..

It will be part of the risk methodology for your company, because remember every institution will have its own. Because remember..

Why don't they follow each other. I have explained the process that we go through the enterprise risk management review, every first quarter of the financial year. The

outcome of that is the risk management report and the risk register, and in that document, the risk for example, the risk appetite, the levels of tolerance, are captured, in that document. And you are saying that as much as they are in that document you want also to have the risk appetite captured elsewhere as well?

No, I am not saying…

It is not supposed to be, it has to be elsewhere other than in the risk management report.

Yes.

And maybe I am saying help me get a sense of what it is, is it a specific provision of the PFMA that says we need to have that, and if so what provision?

It is not a specific provision. I think we can even maybe some other time if you really want to follow what I am saying, but there ..

I still need to get a sense. It is okay, I am answering that to help you finalize your research but if you are asking me something I have never heard of then I need to go and cross this to say this section of the PFMA says…

But it is not a section of the PFMA.

So where are you taking it from?

Remember the enterprise risk management will differ in implementation from institution to institution so now the question I was asking was as far as your organization is concerned, was to say is there a specific documentation somewhere, it doesn't have to be a standalone document, it can be … because like you said there will be the risk register, there will be the risk reports, because those you sort of update every month or every quarter.

No, but I am talking about Tumi…

But I am explaining to you, I will get there. So I am saying there will be the register, and the report and those you can do, I am not sure how often it works here, like where I know for sure at my employment it is every month, the different regions will update their risk register online. So that is just like a live document, ne? And the risk report, however often, maybe it's needed at strategic level, then I can just draw the risk reports for them and give them. That is the one thing. And

then on the other hand there is an extending policy document on risk, that just explains the policy on my employer as a position for them that suits the organization as a policy. And then there is still other documents, which is a methodology, and in that document it clearly states the methodology we apply in terms of using the risk management, but it is not like it is from a section in the PFMA, it is just part of how they manage the risk for their own purposes.

And I think that is where we are talking across each other, because I am saying that the product we come out with, after the ERM is the risk management report and the risk register and in that report, that report spells out the process, it spells out the levels of tolerance, the risk appetite and the detail of the risk register with the detail of what the risks are and what the root causes are where, what controls do we already have in place and what are the additional actions we are going to take. And that document is like, that is a single document that will come up in a year; that is like the high level, then based on that you cascade from the risk register, divisional levels, but I am saying to you what you are asking now, for me is what we have in that report, because we only do that ERM once a year, and that becomes a report for that particular year, that spells out how we went about identifying the risk, the methodology used, the levels of tolerance, the risk appetite and then the detail of the risks themselves and the mitigating factors. And you are saying no, outside of that document, with the risk register I am referring to, you are expecting that to be in another separate document, not this one and I am saying if I need to say do we have that, I would say it is in the risk management report which is the outcome of the ERM which is conducted once a year.

Okay.

So that is not always going to come up on a monthly or bi-monthly basis e.g. we have our risk management committee meetings on a monthly – we have tried to change that to bi-monthly now – but at a board level we report on a quarterly basis through the audit committee and the board, based on that report. That is like, if you were to relate that to the annual business, the annual performance plan, it would be like your risk annual plan or your risk business plan to say this is what you came up with when you conducted the review and then you will report against that, and then we will have covered all these things we are talking about.

I think we…

Where we are not getting each other is I am saying that risk is in that document, that is the outcome of the annual review, and you are saying other than that document you are anticipating it to be elsewhere, what is that based on, and what would that other document be called.

Okay.

…Which is why I say I need to cross reference from treasury regulations or the PFMA because then it means that there is something we are missing.

I get what you are saying because I think this risk appetite thing, in your instance it will come out of that report.

Yes.

I get that, it is fine. I think now what I am also thinking of, because you do have a policy document..

We have a policy document.

Yes, so I think I was thinking along those other standing documents, to say that maybe also in those standing document there will be a note somewhere, not a separate document, but maybe a note somewhere. But if there isn't it is fine, I don't think there is like fast rules that there should be this note and that note shouldn't be.

Okay.

So I think maybe it is something I was just thinking might be there, but it is there and there is no problem. I am sure there will be different ways of doing this thing.

Okay.

We are going to question 5: I want to understand if there is a point before the strategy, or strategic objectives are finalized, if there is a point based on the work that we have already done on your risk document, is there a point where you can say now at this stage we can confidently say we have covered all the bases that we can think of, at least for now – because remember that risks change. So is it possible that at some stage we can say 'now we have covered all the bases for now that we can think of'

I am not quite following the question. I am listening to you but I am trying to read it again, to say on what we have already discussed, because I think we have spent too much time on no. 4 now. If you say is there any point at which point, at the point of formulating the corporate strategy or…

Yes.

I think we have gone through that and I have even gone back to say we do the risk review before the strategy, so by the time we go to strategy we are already basing whatever we are doing on the risk that we have already identified.

Hm. So by that time..

So if you say by that time can we confidently say we have covered the risks..

Yes, I remember I did say to you some of them would be the same but I just need to be clear. Because I might think it was a yes but if you say that, then it is then clear.

So no. 6.

My answer is yes, the risk profile can change, after formulation during the execution, because you do it, which is why I was saying this is almost related to your first question, there is identification, assessment…

And the mitigation.

Ja, and the mitigation, so as to say you would have done that in the beginning of the year, but you need to review that, your circumstances might change during the course of the financial year and then you will have to adjust as well

Yes, that you have also answered already. How often is the organizational strategy performed. Is there a time line, how often does it happen?

What organizational strategies?

The strategic objectives or the strategy?

The strategy is reviewed annually, that is the PFMA requirement; if you are talking the organizational strategy, that is why I am kind of…

Yes, but I didn't want to just take from the PFMA because that is why I am doing interviews.

Ja, how often is the review of the organizational strategies? That is why I am saying maybe clarify the organizational strategies, because it is not organizational strategies, it is strategies: what specifically are we referring to here?

I want the strategic objectives.

You mentioned strategic objectives, they are reviewed annually, every financial year. At the time of reviewing the strategy and the annual performance plan. E.g. if I were to give specific reference to our organization during the first week of July and at management level we work for our own strategy review process and based on that (that is why I am running around now for the packs for the board because next week we are having the board strategy session) – whatever the outcome of what management did at its own retreat is what we take to the board for the board to either agree and say 'take this up' or 'you miss the point and this and that' because as a schedule 3A entity we are expected to submit to the shareholder the first draft of our strategy for the following period, and the annual performance for the following financial year – by the end of August. So that is a standard process. We do it now and August we submit the first draft, November 2nd draft and January the final draft.

Okay.

So you would review your strategic goals and objectives around this time to say are they still relevant or do you still want to retain them or do you want to change them, do you want to add a new one if there are any.

Thanks, I think also that is very clear. Also I want to understand if there are specific steps for your organization, or it is just the management practices that are not officialized, or are the official steps to say when we go for a review, this is what we do, this is the same step we do, this is how we do the strategic reviews.

I think it is almost the one I have just said. We start with enterprise risk management, so that by the time we review the organizational strategy we have already reviewed the risks so that those risks weight is done or the strategic risks identified during that process and they feed in to the process. But in terms of the strategy itself and the annual performance plan, it is a compliance issue, there are guidelines and reporting requirements from the national treasury – over and above between us and our shareholder, then we have even the accolade, they call it the Dear protocol for public entities that report to them, we have that document that also spells out what entities are

expected to submit. So for us it is a process that starts with the risk management that fits in review, that fits into the review of the strategy by management, from management, management will do its own homework and say to the board 'this is what we think, we have reviewed within the system, here we think we need to adapt slightly and or maybe we think this is no longer necessary for us to keep at a corporate strategy level, we are dropping this to the operational level'. And the board says yay or nay, it goes to the shareholder and like I am saying the process from the shareholder, it is a standard process: you submit the first drafts in August, and then anticipate feedback from the shareholder, sometimes it comes and sometimes it doesn't, and ja. But ideally when we submit in August they are supposed to give us feedback for our first drafts so that if there are changes required we incorporate those changes before November because in November from compliance and reporting requirements, we have to submit the second draft and then the final version in January. After the final version, the board will approve the final version in January but then approval is at an entity level; the other approval, maybe the board will endorse subject to final approval. But by the time you submit the last version in January you are not anticipating any hassles from the shareholder because they have seen the first and second draft and also there haven't been any significant changes since that time – at least in the time I have been here. I once submitted the first draft, the difference between the first and the final draft will be very minimal, sometimes it will be a question of saying maybe in the final, with the other years, maybe the other documents, the other performance players, will have the annual targets but not the quarterly targets. So with the changes reporting they will say they are okay with the content but as you submit the final version make sure that you have included the quarterly targets as well – those kind of changes.

Okay, that is also very clear. No 10.

No 9 we have done.

What is the significance and evidence of enterprise risk during the review process?

I think I will really be repeating myself if I answer that as a separate question. Then 10 says does risk management form part of KPIs or job profiles?

Hm.

I am not sure about no. 10, about job profiles.

Maybe in your job description, maybe where it says specifically that you will be responsible for .. or it might not be in your job prolife but in your KPIs.

Maybe KPAs, ja, maybe KPAs and KPIs, especially as much as from the policy perspective and the drive to inculcate the culture of risk management throughout the organization, everybody is expected to do their bit at all levels, but at management levels especially, those things that would have come up with the respective general managers for example, and senior managers, are actually expected to ensure that the risk that fall within their respective areas are managed properly – and that is in line with the risk management policy as well. Obviously the detail of what goes into for example the annual performance agreements of different managers would differ according to the level and nature of their job functions, to say how much is expected of them. But at senior management level and okay, let me talk for myself first, because it is not like I go around and review other people's agreements, mine would have that and my expectation is that any other general managers, executive managers' performance agreement has a risk management element in it.

Okay. That's fine. And no. 11. Here I wanted to get a specific answer in relation to allocation of resources, to say that when the resources are allocated whether it is human or other financial resources or any other resources that needs to be allocated in the organization, is this done in line with a …

Okay, to a certain extent it would affect the allocation of resources, because if you have a standard mandate of what is expected of you but it is not every year that you can be able to do all that you anticipated or needed to do, but after having gone through the risk and assessment process and identified those risks, for arguments' sake, what we have agreed on, even with the risk identification process, where you say for you to mitigate that risk you need to come up with a BCD for activities – some of those activities will require either email or financial resources. So the extent to which you will be able to mitigate the risk as well is depending on whether you will have the resources available. So as we go through that process we go through that, we identify that, but when we start breaking these things down to divisional levels, we for example, if I were to take the financial risk, the one related to the inadequacy of the funding that we are receiving, that ordinarily will fall mainly on the KPAs of the financial officer, but it cuts across the organization. So if we say the grant we always receive from government is not adequate for us to do a, b, c, that is why we also have a commercial mandate for us to be able to generate revenue – which is something else as well because we

actually believe we are not supposed to budget for a profit, for a surplus or a deficit – but we still generate because that is part of our mandate but once we have done that we can't just have 'okay we have generated 80 million this year, we are going to take it and blow it and supplement the government grant' because we actually a 3a entity, we still need to go back to government, national treasury, and say 'can we be allowed to retain this much?' – because otherwise it is supposed to go back to the fiscus. So we need to go back to treasury and say 'can we use this, these are the key strategy programs we have identified in which those funds will be spent' and the treasury has the right to say yay or nay – so far we have been lucky in that the few years that that has happened there hasn't been a time when they have said 'no, we can't keep it'. So what I am getting at is once those resources have been identified we need to generate, the grant is diminishing, we need to in terms of buy our commercial revenue generation initiatives, but for us to be able to do that we need to beef up our capacity in-house. So for example when it comes to the fight of the resources and both financial and human, if we say we need to generate more commercial revenue to supplement the grant, then we need to beef up the structure for the commercial we need, so there are more people who are hands on and driving the commercial element. So if Zandi needed a vacant post that we need to fill but in terms of the commercial element the question would be 'do we fill in Zandi's one or do we prioritize the commercial one' because we need to identify that and maybe put that one at the back and prioritize the other. So that is the allocation of resources.

Thanks. That is also crystal clear. The last question, can I just explain it?

Who wrote it, because the person should have seen that the questions were not ambiguous?

To me I understood it because I am the writer of it, but when someone else reads it I realize it becomes a bit… because I read these things every day, I assume that every person will be able to understand. But if you understand it, perfect – otherwise I can explain it.

Let me try and explain, the more I read the more it is not saying anything I can understand.

(laughs) Okay, let me explain then because I might be wrong but my understanding is that your organization used to comply with other rules, international rules and all sorts of rules that you need to comply by.

Ja.

At the same time you here also create some rules for your stakeholders and clients or whoever you supply information to – that you expect those people to abide by. So there are two sets of compliance, I am talking about the compliance you need to comply with, from outside, and the compliance that the people you do business expect you to comply to – your own rules. So I want to understand now the extent to which this risk management initiatives and the systems in the organization, how do they help you comply both with the external rules you need to comply to, and with the ones that your own people, your own customers need to comply to – that you have created for them.

Can you separate… it is still so confusing. I understand you need to check compliance, that whichour organization needs to comply by.

Ja, let's start with that first.

And then you want to know..

.. the ones that your organization created.

.. by our stakeholders.

Yes, that you have created for your stakeholders to abide to also.

Ja, and the question is…?

I am not sure if it will happen but if it does, how is this a risk management system that you have at the moment helping you to comply on both sides, to make sure you comply with the international rules and to make sure that the people you expect to comply to your rules, also comply. I want to know if it has any effect, or not really.

It is still a bit complicated for anyone to have a simple answer to, because for example compliance in general would … that there is compliance by us that comes out of us being a Schedule 3A entity, from the SA Government perspective. But because we are part of the international board , then there are other compliance requirements that come from the WO, from the International Civic Aviation Organization, that is linked to our provision of information and all that. As far as we have to comply..

So that is the second leg of compliance. The first leg is the schedule something you talked of and then there is the international regulations you need to apply by.

Ja, and the risk identification process and the risk management processes that we do – which is why I said when you said what forms the basis of the risk identification – I said for me, on top of the list it is your mandate, what is expected of you, what you need to do. Because here we have a mandate from the South African government as an entity and we need to comply with that. As an organization we belong to international bodies and there are regulatory requirements that come to us because of our association with those bodies, that won't apply to any other Schedule 3A entity that does not belong into those bodies. In the process of the risk review we take our mandate and say who are we, what is expected of us and at a national level, as a schedule 3A entity, this is what is expected of us, but because of our links with those other organizations, this is what is expected of us: what are the risks associated with all that which we need to do – and once we have done that, the risk register, the top risks which we come up with eventually, we would have touched on all those elements.

Your compliance, and..

Ja, what we need to do here, and if we need to do this what can stop us from doing that, what can stop us from achieving it. So the risks would have identified all those elements and take them into account and what we normally say about compliance is are you dealing in an ideal world – it is either you have to comply or not comply; you cannot half comply or comply 80%, but in a real world, you end up 80% because of these risks and some are external to you.

Beyond your control.

That is beyond your control so you cannot do all that which you wanted to do so as your targets for this year you are going to limit your targets to this based on the resources you have at your disposal, because for you to be able to do that you would need these resources. So based on that the risk management processes will filter throughout your mandate for the stakeholder, both at a local or domestic level within the public sector and with whoever you associate with outside. And that I am linking both the domestic and the international as far as what we are expected to comply with. But in terms of any other stakeholder we establish partnerships, then we will have an MOU for argument sake or a Memorandum of Agreement, as a particular party, with

the suppliers, but that is still linked with our compliance because for us to be able to comply in the first instance with the PMFA and the treasury regulations, we need to ensure that the manner in which we do business or engage with our stakeholders, that is still in line – so that we maintain our adherence throughout to our own compliance requirements. So it would, it is just that the question is…. ja, but the risk management element will affect or will improve the manner in which we comply.

Ja, your compliance levels. Okay, thank you very much, I think we are done with the questions.

Okay.

ENDS.

9.6 2013-08-11-16h00 Interview

We are going to start with the first question: so just to explain, I have made a list of questions but it is just an indication so you are allowed to answer any question from whatever angle that makes you comfortable. So I am going to start with the first question, it is the semi-structured interview so the questions are just a guideline, you are welcome to say as much as you want to say.

On question 1, I have broken it into three sections because when I ask it the way it is it just gets too much, so I am going to ask the first part of question 1: What forms the basis of risk identification within your organization?

What we usually do only at the basis, you know our organization is a state-owned entity, we are governed by PFMA, and also in terms of the requirements we also as we submit our strategic plans, we also need to submit our risk management plan to the shareholder. So that is legislated, but it is also important for us as an organization to understand what are the key risks that happen, that we need to manage.

So what we do, what forms our risk identification, we start to also ask the board what are the key risk areas that keeps them awake at night, and then working together with our internal auditors, we sit down and establish a risk register to identify the top – we call them the top 20 risks, sometimes it is not 20, it can be 15 or 10 enterprise risk, and from there we do the analysis looking at the likelihood of the identified risk and the impact of that risk and what are the controls in place to minimize that risk and with those controls are you able to say you can reduce it and look at the residual risk and decide some of the risk you can insure them and some of the risk you have to accept that is the risk, it is inherent risk of the business you are in - but to try and minimize that. That is one area that is important for us when we identify risk. The other one we are a 24/7 essential service, we cannot afford not to have, to provide the service to the South Africans. So it is important for us to have a strong business continuity in place and it is a service deduction and a disaster risk management as well, response, how are we going to respond to certain things. So with a business continuity plan that is more on operational level, to say to minimize the risk here, if anything can happen to this organization we need to have another place where we can still have the services.

So we identify the key competencies that are required, key infrastructure that we need to have, in making sure there is a duplication somewhere else, where if anything happens to let's say to head office, we are able to work let's say at the airport, or we

are able to work maybe even outside the country. So that is how we manage to identify that risk and then we have on a yearly basis a risk register and then we review those risks that have been identified. Then we take that to the auditing risk committee, they look at that and recommend to the board for approval. So then you get another second chance to take it back to the board, and if the board at a strategic level feel there is another risk that we have not looked at and considered, that is when they come in to say let's add in this maybe in this area. So that is how we look, we identify the risk in the organization.

Okay, before question 2 I just want to confirm question 1, that we have covered the risk identification. I was also going to ask you on question 1 relating to the risk assessment, but from what you have explained you have already covered that. So I am going to move on to question 2: how do the organizational risks get integrated and encompassed into the formulation of strategy or your strategic objectives? So in other words I just want you to…

I understand. What we do is that when we do the risk identification for our risk register, we identify the risk and then from there we say in terms of the strategy in the strategic objectives that have been set up, these risks, which of these key objectives that it will have the most impact, and then we link the risk to those key objectives or goal. Although if you look at the total risk identified all of them will have an impact on how we implement our strategy and in a manner that is successful. So that is what we do, we have the risk and then we have the identified objective, link the risk to those objectives that if this risk is not minimized we will not be in a position to achieve these objectives. So then we link the two in that way. And then from there when we do, because we do it on a yearly basis, the risk identification, then we prepare and develop our strategy, strategic plan, we also incorporate the risks that have been identified that year in our strategy. And then saying how are we going to make sure that we minimize this risk and how are we going to deal with it and how are they affecting the whole strategic direction of the organization. So they become part of our strategic plan. So if you read the strategic plan there will be an area, a section that talks about risk and how we are planning to manage those risks and how they are affecting the achievement of the objectives as well.

Okay, I understand that.

And then when it comes to operational plan, with the identified risk register we sit down and really look at the risks itself, as I have said the controls that are there, what are the

additional controls that we need to put in place. if we put those controls how big is the risk then going to be. Then we allocate different divisions to different specific risk and then they take those identified actions that needs to be taken to start and come up with an operational plan in terms of managing that risk – because some of the management of the risk might be in finance department, or let's say in supply chain, where we need to have an insurance company that is going to insure our asset. So the asset manager in supply chain needs to be in a position to identify all the assets, the asset register must be updated, and all that. And make sure that those risks are…. If it is an issue, if the risk is security of assets then we look at the kind of security system that we need to have in place. Then it will be the responsibility of facilities manager together with the supply chain asset manager working together, coming up with an operational risk plan to deal with that. So ja.

I am happy with no. 2. Question 3: How significant is the role of risk, like the risk concept, the whole risk system. How significant is it?

As I have said to you, the board takes it very seriously. I think was it four or five years ago we didn't really have a risk committee in place, so we realized it is something that is very important for an organization, so we have put the risk committee; all the EXCO members are members of the risk committee and the CEO is the chairperson of the risk committee and then in each division they also need to have their own champions, however with the board as well, the auditing and risk committee has taken issues of risk very important, and in fact for King III as well, we need to be looking at this. So what we do, after we have submitted the risk register and our internal auditors when they do their three year internal audit plan, they are doing a risk base, so they cannot do the three year audit plan without working around the identified risk. So that is how significant it is. And as I have indicated, we also need to submit to the shareholder as well.

Ja, I just want to follow up on one point you were making about the internal auditors: who does the internal audit for this organization?

It is external, PWC.

PWC. So just clarify to me their role in the…

In the beginning of the year, before they start with the year risk, the internal audit plan, the three year internal audit plan, they sit with us and we sit with the executive team and together also with the board, we ascertain the risk, we identify the risk together –

the top 20 risks – and then look at the controls that are there, agree/disagree in terms of those controls and then they will take those identified risks, link them to the objectives of the organization and then come up with a three year rolling internal audit plan – which the board will look at and then the board might say there is another risk that you are missing which we would like to play part in it. The role of the internal auditors as well is that they need to also give assurance to the board in terms of how the risk is managed within the organization.

Okay. I am happy with that. Question no. 4: Does this organization know how much risk it is willing to take? So I need information the risk appetite or the risk tolerance of this organization. Is there a policy that speaks to this and if there isn't a policy I just want to know what is the understanding of the organization.

This is an area where I would say we still have a gap. In fact when we were having our last board meeting, it is one of the issues we have discussed with the board, to say we need as the board to identify our risk tolerance and the risk appetite; we are not yet there. However we do the materiality framework which we use when we are dealing with some of the risk. We look at if this happens that will be catastrophic, and if this happens that will be significant, if this happens it will be medium, and then these are minor issues. But the gap around the materiality framework that we are using is so linked to the revenue that is being generated, that comes in within the organization. So for me it is just not broad enough. But we are using for now the materiality framework. But in areas where there is no policy specifically that is dealing with the issue, that is where the gap is. But in areas where we can insure, we insure.

Ja. I am happy with that. No. 5: I want to understand if there is a point before you finalise the strategy where you can confidently say that you have covered all the bases in terms of what you think are the main risks. Can you say this is the strategic objective we formulated, and we think these ones have considered all the possible risks, the way the strategies are set out.

You see Tumi when you are dealing with risk management for me it is usually a continuum. Yes, you have got the process of starting identifying the risk but during the year as you look at the controls you have put in place and coming up with a risk management plan from the different divisions, you might find there is something you have missed and that is then an opportunity for you to go back and look at that. You must remember what we also do is take our risk plan and update the risk committee in

more detail now twice a year, for them to look at it. So basically there is an opportunity to re-look at your risk and also when you review your strategy as well.

Because earlier you said you review your strategy once a year.

Yes.

And now I want to understand, the risk registers and the risk management system, how often do you review the risk register?

The risk register we also review once, but it does not mean that if there is any other identification – like now, we had a session with the board where the board felt that we need to go back and re-look at the risk and at having an additional issue which the board feels is a risk. But in terms of the process itself the risk identification is done once a year, then we work with those top 20, but now we have around 15 risks, and we work with those. But if it is something that is coming up and becomes like last year, we had an issue where we thought we would be getting money for the high performance computer, the other year, and then we didn't get the money from national treasury. So it started to become a huge risk for the organization. So we had to go and put it in the risk register as a key risk because we didn't have back up and all that. And then a year later we managed to have that.

Because I think what I want to get to is I understand very clearly that at the top level, at the board level, it is strategy, the risk is done once a year, but operational?

At operational level it is part of what they need to be doing because every month we have got a risk committee.

Yes, so they have those monthly…

Yes, so the identification of the risk, you see your question around the risk profile and formulation, the risk profile and formulation is done once a year but management of the risk is a continuum. You see?

Ja.

So we have the risk committee that meets, but the management executives meet with their teams so that they prepare for the risk committee on a monthly basis.

Okay. Question 6 I have also covered. Can the risk profile change after formulation during the execution and what would happen in this instance, just to make sure, you said of course the risk profile changes all the time, risk is managed operationally all the time, and when the risk profile changes then the strategic objectives when the meeting happens once a year, will be aligned to the risks.

Yes. You might find that sometimes some of the risks that you have identified is already aligned to one of the goals, or it is affecting all the objectives anyway. So you know, like I am talking about the high performance computer where we had a challenge, I mean IT is an enabler for the organization, so it means almost all, even the service delivery for the weather service, will be affected. So we had to even take it up with our Director General Department of Environmental Affairs and the Minister. Then national treasury gave us money, they gave us R50 million for the high performance computer. But if you look before that, it was not put in as a key risk and then we realized as we worked with the risk committee that this is a risk, let's take it up and bring in the board and the ministers.

I understand that. Some risks come straight from the top, they will be identified from the top. Some risks will be identified from the bottom, maybe from operations and their divisions. I want to understand how the emerging risks that come from the bottom and the ones that come from the top, what is the process, how do you link them?

You see what we do is to identify the top risk, the top 20, then as the risk committee which is made up of the CEO and the EXCO members, take those risks. E.g. there will be a financial risk, and then the sponsor for those financial risks and maybe risks associated with supply chain, the CFO will take those. Right? He solely will have the responsibility of making sure that he puts those controls. Then if the other risks are operational the operational GM will take those and then if they are HCM then the HCM will be the sponsor for those, ne? If they are let's say related to governance our company secretary will take the lead for that. Then when we have finished doing that, each division will take, let's say we have identified 15 risks, when they develop their own divisional risk management plan, they are going to say this no. 1, what are the controls that our division is responsible for, for this risk? How is this risk in our operation, how important is it and take it let's say a level lower, and then what is it that will need to be done by who and by when.

So you get a date.

Yes, so it goes like that. So when the EXCO comes and reports, he reports in totality of his unit. Those key risks like the financial ones, we need to take insurance, okay fine. But then there are other risks. And then if the issue is human capital, as much as ACM executive is responsible for coordinating, putting policies and implementation of policies within the organization, e.g. our CFO is also responsible for commercial and we are just establishing that unit. One of the risks that was identified is that for commercial to move faster (commercial is moving very slow) because there is no established structure. So you see you have got the sponsor in terms of HCM, in provision of the structure that is required. However the person who is accountable is the CFO. So you will put the CFO there and the CFO sets the time lines by when this needs to be done. But the support team department is HCM. So all of that comes back to us and our risk officer will monitor the time lines that have been set, what are the things that are moving, what are the things that are still behind, and that is a risk on its own.

So what level is at, at the GM?

No, it is not at a GM level, it is at a senior management level, however for the moment we don't have enough funds, our company secretary is doing that. So it is at a very senior level.

I am happy with that. I think question 7 we have also answered, it is asking how often can or is the organizational strategy performed.

We have very clearly said once a year, ne?

To align to the changing risks, ne?

Hm.

So question 7 is clearly covered. What are the specific steps involved during the review of the strategy? Remember based on the changing risks you might have to review the strategy, the strategic objectives. Was there ever a situation where you had to review the strategy?

There was not, no, not yet.

So the strategic objectives have never been reviewed?

No, we review our strategic objectives on a yearly basis. But it does not mean when there is another risk we need to go back and review the strategy.

Yes. So you just review the… okay, maybe just explain to me what the process of review is.

Review what?

When you talk about you review the strategy.

No. You review the strategy, when you do a strategy review we look at the environment and what needs to happen. We also during that time, remember I said we also look at our risk register, based on the context and the issues that are out there that are affecting us. And then we must remember, the strategy is a three to five year strategy, so when you look at enterprise risk you look at the enterprise risk at a high level. So then you need to really analyze what are those key risks that are affecting the organization. So when we do the review of the strategy we look 1) at the priorities that the government are putting in place – is there a change from the previous year? No. Is there a risk for us not to deliver on what we need to deliver on? Yes / No. Is there an opportunity for us? You know? And what is the risk of not maybe getting that opportunity. E.g. now we have the national development health plan strategy and in chapter 5 they talk about establishment of a climate change centre. For us we have put it in our strategy, it is an opportunity, but it can also be a risk, because it is an opportunity for us to take a lead as that climate change centre. However in SA there are a lot of other organizations that provide similar services like us, you see, there are research institutions, we are the custodian of scientific information and the relevant services. So there is a risk that there will be some competing institutions that would like to take the lead in there. So that we have put that in our strategy this year, to say this is the risk that is there however it is also an opportunity for us. How do we start to come up with a process? So we agreed that we are going to start engaging the department e.g. now we have a workshop with all the other players that are playing in our field , to look at what kind of a framework or coordination that needs to be put in place. So we have started to position ourselves, you know. Last year if you read our strategy plan we didn't have anything that talks about positioning in terms of climate change but because there is now a new initiative by government we need to be in tune with that.

So you actually do the strategy plans.

The strategy plan of the organization, and factor in this issue: It does not mean sometimes you have to change your strategy though, you can link it. E.g. we already have a strategic goal that talks about climate change and climate variability coming up, so we have put it in there; we have identified the risk but what actions do we need to put in place to manage that risk. We have done that. but that is at a strategic level but you must remember that at an operational level there are a lot of risks that keep on coming, which you need to act on, which cannot wait for the strategy review, so that is the implementation part. E.g. when we had one of the… we are sharing the big things there with other companies, and the landlord was renovating another block and the security was not there at the security gate and people came in and stole two cars, at the Weather Service.

Which is it?

The building next door to our building.

Head office?

At the head office. They were renovating there, but usually there is a boom you need to go through for the whole area, but that boom, there was no… they opened it up because there was construction and all that, so at our organization I am sure when you came now there is a security again that you need to go through.

Ja.

And then also at the reception there is another security. So we had to… we couldn't wait for the strategy, you hear my point, to beef up that security to manage that risk. Although the risk in terms of security of asset and human capital of the organization is there at a higher level, that risk has been identified, but in terms of what is happening at a lower level and the actions that we have put in place, they were at a higher level, but something happened at a lower level which we needed to act on. So that is what happens.

Ja, it is continuous at the strategic, at the operational level.

Ja.

So we have covered no 8. No. 9 we have also covered. What is the significance and the evidence of the enterprise risk during the review of the process. So when you do the review you do the risk both at operational and strategic.

Yes. What we also do as we look at that risk, is to say okay we have identified this risk, we have put these controls in - let's say last year – are these controls adequate to mitigate the risk? If our answer is saying yes and if it is saying no then we start to ask ourselves what else we need to do, what additional controls do we need to put in place. But there is a school of thought that the way that we manage the risk, we manage the negatives, and forget about managing the positives.

I agree.

So I think as we improve we also need to look at the positives, but here and PWC we are using the ISO approach which is more emphasizing the negatives than looking at the other. So probably with them we need to just re-look at our methodology. Also we might miss a lot of opportunities and that is a risk on its own!

Yes. Because the whole risk management thing is intended to, in as much as you are looking at what could go wrong..

It is to look at the opportunities.

Yes, because for everything that may go wrong there is also an opportunity. So everyone that you look at as a risk like that, the example you made earlier of the climate change, you talked about the risks very well but also about the opportunities and all the risks I can tell you now, if you go through, there is also an opportunity.

Ja, I think the methodologies that are there have been emphasizing the negatives, even the way that you craft the risk, you say 'the lack of' and you find that you don't have a lack of, you do have human capital, however… you know?

Ja, because sometimes you mustn't say lack of, you must say inadequate blah blah.

But sometimes it might not be inadequate, it might be how you utilize. Ja, but anyway, it is a discussion for another day.

Yes. So no. 10: Does risk management form part of the KPIs?

Ja.

From what level?

If you look at our strategy itself, no. 1 we need to have e.g. if you look at the strategy and you look at one of our key objectives, it is to have an unqualified audit, clean unqualified audit. And then there is a column that talks about the program activities that need to be there. Risk management is in there, as part of the strategy itself. So when the auditors come and they are looking at auditing us, for us to reach that key performance indicator of having a clean audit, we need to make sure that we manage our risk effectively and efficiently within the organization. So yes, it is linked, and then from there it is going to move to the other levels. But at the moment it is up to the level of the senior management. E.g. I talked to you about the business continuating, so there are objectives for people who are responsible for that.

Fine, so before we move from no 10, the KPIs, at the manager and senior manager actual performance agreement, do they have clearly where…

No, it is linked to certain goals.

So some of the activities that they must do.

So you must remember our… if you look at our risk plan, the risk register, the risk plan that we have, it will tell you that this objective is linked to this risk, this risk is linked to this objective. So even an individual doesn't reach those indicators, aligned to that objectives, maybe some of those risks have not been managed well for us to get there.

Okay, I get that. The allocation of resources. The risk management system in the organization, how is it helping to allocate resources, whether the resources are human or non-human?

How does the risk management system affect the allocation of resources?

I have indicated to you, one of the things, the challenge that we have at the moment, is that I don't have enough funds to have a risk officer. So for now we have utilized the resources that we have in-house, the company secretary in terms of our governance. Our governance is at a mature stage, the system is working. So we have got that. but in terms of allocation of resources at the moment, it is one of the areas where we still have a challenge, because some of the people in some divisions tend to have some risk officer or owners, all the managers need to be risk owners, but you also need to have, I believe, that you need to have a coordinator for each division. That we don't have. So each manager is a risk owner, but each division does not have a person who

is coordinating and managing that risk. Maybe at a lower level, collecting and doing all that. That is no. 1.

The other resource we don't have, which I think we just need to get to the stage of maturing our risk management, is to get software that will make it easy for everybody. That we don't have as well. So we are still busy in Excel.

Happiness. The last question: I want to understand, say this is your organization, and it is governed by some international laws from everywhere, so this organization needs to abide by those laws.

Yes.

At the same time, the very organization might also have laws that pertain to the service providers that this organization deals with. So does the risk management system help you to be able to comply with these international laws and also does it help you to manage the laws that you want your stakeholders here at home to deal with?

Ja. It does in a way because when we look at different risks, identifying those risks, we also look at issues in terms of compliance – like I remember the World Organization, they have got their own standards that we need to meet; the International Civil Aviation Organization, it has its own standard that we have to meet. Our act itself, when it comes to the International Civil Aviation Organization, has given us a responsibility of being an authority, where it is looking at all the airports, whether they are complying with the requirements of the international civil aviation, the infrastructure and all that. So by virtue of that, I think you have interviewed Beki, he is an independent body within the organization, that is doing that, and also doing audits. So he has a responsibility to manage that risk for the organization. So there is that link and the activity, because he is also responsible to do the audits. So as he is doing those audits based on some of the identified risk they are linked to his audits he is doing. E.g. if they identify that some of the airports are not using equipment that is not up to the ICAO standards they need to inform the civil aviation organization. So the issue of risk management, is part of what we are supposed to do on a daily basis because our job is to protect lives and property – even life at sea. So it is also embodied in what we do, in terms of the standards we have set. But also when it comes to aviation it is one of the key clients we work with, we have service level agreements with them where it is all stipulated what is the service that they require from us, but added to that we also have ICAO, and

that is where the standards are actually set. So what Gabo does in aviation when she is developing a risk management for aviation, a management plan, she also looks at those things, to say when it comes to human capital you might have an executive that is heading human capital as a sponsor, but the risk owner is Gabo at aviation because aviation says people need to be trained, they need to have these kind of competencies. So if those competencies are not there, there is a risk that SA service, ICAO will say SA cannot provide certain service. So it is a risk on its own. So then Gabo in aviation needs to make sure that those people are trained to the required standard. So when it comes to HCM, human capital key risk competencies, of a certain standard - that is what is required. Then she deals with it.

I think we have covered all the questions.

Ends

9.7 2013-08-12-09h00 Interview

So as I explained it is a semi-structured interview so you are allowed to answer it from whatever angle.

Sure.

There is no wrong or right answers. So question no. 1: this is all related to risk management in your organization as a public sector institution. In your understanding, what forms the basis of risk identification in your organization? Where would the evidence be and how would you identify the risks?

That there are risks in certain areas?

Risks – risks to the strategy. Remember this organization has strategic objectives, so from where you are sitting you do influence one way or the other those objectives.

Okay**.**

So from your side, what will be the basis of the risks that you would identify?

Well as it is part of our division called operations and operations has a committee that deals specifically with risks. Obviously before we take those risks to that committee we would have identified as the ICT team, with ICT managers and including myself, determining what we see as risks or not - and the level of that risk. Obviously the important thing there is your understanding of the environment, knowing your operations, and obviously before you even do those operations in any case, you know that they are linked to your strategy because when you set up your annual plans and your operational plans you do as much as possible to link them to the strategic goals and objectives of the organization. So I think in our case we have got that linkage of a number of committees and processes within the organization, to use as your basis for identification.

Now those committees you are talking about, where would they get their information from?

What kind of information?

The risk.

The risk is identified in that particular area.

Oh, they identify the risks.

No, in the committee, they would then discuss risks from each area within operations. E.g. we would have identified the risks within ICT. So the important thing really is to at that level of committee, is to determine the seriousness of the risk, or even discuss whether it is indeed the risk as identified by a particular unit within operations. There will be instances – and by the way I am still new here and I have only attended one of these committees - but I imagine there would be instances where the committee itself says that this for instance is not necessarily a strategic risk, if we are only looking at strategic risk; there is a tendency for people to want to take anything into a risk register, so like one of the roles of the committee is to determine whether indeed this is deserves to be there and classified in that fashion. Most of the times risks are varying, like you are saying, according to classifications you would have your strategic risks and so on and so forth in IT, and like adding other things, like vulnerabilities and so on at a much lower level, and as an IT person I may take something that is too low level to be highlighted at that level, so that the committee's role is also to determine those kind of things.

I think that is understandable. And then also the assessments of those risks happen in that committee also?

Well yes and no, because the committee does look at the progress, you must remember that when you set up a risk you also put in controls and so on, so part of the assessment is really to look at how much progress you have made against those controls. So the progress committee would like to know how far you have gone, so that is one level of assessment. But as you put in controls at a unit level, e.g. at an IT level, as a senior manager for ICT, I would like if we have started addressing a particular control I would like to see the progress of that control. But specifically to ICT we also have a steering committee which is ICT steering committee where we also do our risk, we look at our risks. So like another control or another monitoring happens at that level.

Ja, so that is your own ICT, before it goes to the other risk committee.

Well the frequency of the ICT steering committee now is such that we are doing it every month. So we discuss all sorts of things there, every month. So sometimes you might find that we are discussing things that already come from the committee or EXCO have highlighted and sometimes we are discussing things that emanate from this side. So the direction of the interaction of the flow of information sometimes may be not so

much that it has to go there first before it is discussed as well. However on the risk side, the final on what risk should be addressed and looked at, is not the steering committee; the steering committee can advise in terms of what steps should be taken concerning that risk, or even the identification that we talked about earlier – they can advise but when it comes to risks, to risk management, the committee that is responsible for that is the risk management committee.

Okay. Still on question one, because I just broke it down into risk identification and assessment, and then the mitigation plans also. I guess those will also stem out of the.. when you see there is enough controls or not really, then you will come up with action plans.

Ja, well again, the process of risk management sometimes I think, because it is so structured you are required to at the very beginning, come up with mitigation plans and so forth. There may not be adequate when you are still doing them just at that moment when you are required to do a risk management plan, and may need a number of rounds of refining and so on. But ja, like I am saying, those mitigation plans must be up there up front, but a refinement would still need to be done – either in the steering committees, or even within ourselves when we look at it and feel that it the control we set initially was the right one or the mitigating factor we said was the right one or it is not and is not working.

Okay. I think we have covered the first question. Question 2: How does the whole risk management system get integrated into the formulation of the strategy or the strategic objectives – even the operational plans? Could you clearly give me a link from the risk assessment and the methodology that is in place, to the ops plans to the strategic objectives?

Ja, well it is a link that I can draw to you on the basis of my experiences and not necessarily that we have a chart in the organization saying that I move from there to there to there. It probably exists but I have not seen it, I have been here three months. But the linkage is simply based on the fact that like I said initially, everything is linked whether we are…. The linkage on our operations, there is that first link between the strategy and the operations that is done through your normal annual planning process, strategy planning, which then emanates down to your operational plans. But it is those operational planning and those various units, say IT, that you then on the basis of the stuff you are going to deliver, identify those risks – those risk areas. Now the linkage back again, to say okay if I am addressing that, like I am looking at that particular

operational activity for this financial year end, and I am identifying risks for those operational activities, to which part of the organizational strategy is that impacting on? So for me you would then have throughout your planning process, have that linkage. In fact risk management in my view, is part of all of the planning process – whether you are doing strategic planning, in the end everything has to talk to each other.

Ja. Okay. Some of the questions will look as if it is the same thing but I just want for academic purposes to clarify. Okay question 3 you have sort of answered also, but in your assessment, how significant is the whole risk concept towards the setting of the strategy?

It is very significant, like I just explained it by way of an example.

Ja.

There is here in the list of strategic risks that we have, there is one risk where we are saying that the risk is inadequate, the funding we get from government. Now when you are putting together a strategy, if that strategy is not adequately funded, obviously you are not going to be able to delivery those things that you want to deliver. Now, you have identified that as a risk, maybe again this is where my short stay in the organization fails me, because it is difficult for me to know at what point was that put in as a strategic risk: was it at a time of putting together the strategy, or was it something that because of the disjointedness of putting together, of developing a risk plan from the process of developing a strategy, then it was on the risk plan but not on the strategy side. But for me that is a simple indication that the two should be very much linked - and almost go hand in hand.

Hm. Okay, I am happy with that. So done question 3. Question 4: I am not sure if you are familiar with this one but just explain it to me the way you understand it – the risk appetite or risk tolerance, does your organization know how much risk it is willing to take? Do the officials here know how much risk appetite the organization is willing to take?

Um, okay, the way officials know that I think it is difficult to us to have that kind of thinking, to have that mindset of risk appetite and risk tolerance – well maybe risk tolerance because that is about how much can you tolerate under difficult circumstances, or under risky circumstances. But to say that I can take this risk or move out of our zone and take particular risks, it is not a mindset that is there currently in the organization. But I think it is being developed towards that, but also there is a

good reason for organizations such as ours not to have that mindset: someone who takes a risk takes that risk because they have a whole lot to gain out of it. Now partly an organization like ours is not out there for gain of any sort, even when we talk about the commercial element in this organization, when you are referring to cost recovery rather than making profit. So the moment like there is not much for you to gain something, I think it destroys that appetite! (laughs) So it is a question of mindset, but it is also a structural issue that the organization is not designed to have that kind of risk appetite.

Okay, because I am just wondering. Yes I agree with you that an organization like this is not there really to make revenues and profits, it is more on the cost recovery. But wouldn't we say that still an organization like this would want to take a lot more risk, just in order for it to be able to ..

…to thrive.

Ja, to put whatever mandate that was given to it, to do it in the best possible way?

Sure, no, certainly. There is an element of risk taking from I think an operational side of things, for instance we have got people here whose work is to do research, but those people are also competing with universities and other research institutes like CSIR. I think there is an element of risk taking that needs to happen and not do the same old research that you have been doing, instead looking at other things: there is an issue that we want to remain relevant as this organization, and the challenge about that is that there are people out there who are for commercial reasons, purely commercial reasons, coming into the weather space and coming up with products that are developed to satisfy new ways of looking at weather, to satisfy mobility that is out there – your I-pads and your smart phones and other mobile needs that we currently don't have. Now you need someone who is going to then say: 'As new research that we have to conduct, maybe like something, an R&D, some organizations will call it applied research – we don't necessarily do that kind of research – behind you need a new kind of researcher to do that kind of research work, you need to get the kinds of people that are employed by commercial organizations and in order to come in and shift the mindset into these new types of research. So to a certain extent, yes, we do need to take risks I would say.

Okay, I think I am happy with that. Question no. 5: Do you think it is possible when you are devising your strategy objectives to get to a point where you say 'You know what, these are our objectives and at this stage we think we have covered all the bases risk-wise that we can think of. So at this stage we are happy'. Or is it not possible to get to that stage, to say 'Based on what we know now we have covered all we could think of, so…'

Theoretically it is possible but as it happened – no – not in the strategy session that I was involved in here, not in all the other strategic sessions that I have been involved in, in other organizations. So it would be a great thing to have but unfortunately it never works that way, even with guys who pretend that their processes are, I don't think they actually are in that manner. But the other thing is once organizations have started functioning and have developed cultures, have developed processes, people start working with the knowledge, like situational knowledge, there is a lot of that in the employees of the organization – things like strategy development, risk assessment, are all based on that institutional knowledge rather than people actually sitting down and doing a very hard task of looking at the strategy and risks and so on. It doesn't happen like that.

Okay. So I just want to get this clear: what would prevent it from happening like that, because I am thinking say for instance we want to come up with objectives for the next five years, and we are saying this is where we want to get to but if this is our objectives then the following risks prevail – all the risks at that point in time, knowing what you know at that point – then you can come with all the possibilities of the risks that may come up; meaning that at that point in time you have to be able to say 'okay, at this stage we have considered everything, we are good to go'. But are you saying you don't think that is possible.

Maybe what I am trying to say is that we do it, we do that, everyone does it, but I have looked at strategy documents of organizations that I have worked at, and every time I go back to that document there are things that I look at and I ask myself ' how did we put that thing there?' – that is what I was referring to about the situational knowledge. Like there are things that we put in… I think the process is not an involved one when we do these things, so yes we do it but are we putting things there that make sense or are we putting risks for the sake of putting them? Like I would ask you to check the five previous risk registers of the organization and I bet you for the last five years in most organizations, if they had ten risks in each year, 8 to 9 of those risks are basically the

same. They may be worded differently but someone is saying exactly the same thing. So you ask yourself 'how much do we really apply ourselves when we do these things?' So for me it is the quality that I am saying that it is not possible. The compliance with it oh yes, we can be happy and pride ourselves that we did what the great specialists in risk management and strategy development are saying that let's put these risks up front, yes. But then I mean if they don't help you take the organization forward you have just complied but you haven't really produced a quality thing that is actually…

Hm, and I think you are correctly putting it: I think it should not be about just complying, it has to be about applying ourselves to come up with things that really are real risks to the strategies, not just for compliance purposes.

Yes.

Okay, so I understand that. No 6. You have got it?

Ja

I think we might also have touched on it while we were discussing, but maybe again just for clarity purposes, I am asking can the risk profile change after formulation, during execution? So you remember you have your strategic objectives there and then you have your risk profile at the time to say these are the risks. So this risk profile can it change, and if it can change what happens when it changes and what happens to the strategy objectives also when we change?

I think the changes, if the change is due to the fact that you are still trying to ensure that the objectives are met, there is no reason why not to change the risk profile. The objectives are the objectives, they remain, well unchanged let's say, in view of your mitigating risks or taking corrective actions to correct what you see as a risk situation. Or even to a certain extent saying that our response to that risk, or it is no longer a risk anymore. When it is no longer a risk well and good, then our strategic objectives are going to be met. So I don't think the process of changing the risk profile should have a negative impact on the strategy goals, unless it is changing it for the worse: if the profile is such that you determine that you know we had said we could meet against that thing for us to achieve a particular goal and we realize that you can't do that – at which point you also realize that therefore by implication, you are not going to achieve your strategic goal. And there is no reason for you to still have that objective or goal

there. Or key performance it may not necessarily affect your goals per se, but the various key performance indicators that you have put under that goal. So there is no reason for you not to change on that side if things on this side are not working and I think our performance management system does allow us to change things that we have planned for – for whatever reason, for good reason actually, not for whatever reason, but for good reason you can change that side.

Are you saying the strategic objectives won't change?

No, like I am saying, it depends. They might have to change in my view again I am just saying my views here, but at the same time I think they are very much in line with the performance management system that allows you to review. Look the strategy on its own, the strategy development process where you develop a strategy over five years but review it every year, that review process is a chance for you to look at whether things are still relevant that side and one of the inputs to checking out whether things are still relevant or not, would be your risk profile that has to be taken into account. So yes, in my view change can be done at the goal setting side as well.

Okay. I get that. How often is the review of the organizational strategy… I think you have answered this one.

Ja, it is annual.

It is annual. And are there specific steps that you are aware of, that the organization or the executives or you guys would go through when you review the strategy or is it not any step by step thing, it just…

I am not sure whether it is documented here, but the usual way of doing it is to within the units give input, I belong to IT for example, so within IT I will give input that goes into an operation's divisions input into that and that would then be consolidated under operations and other units would do the same. But at the end of the day we attend a facilitated strategy review session by an outside person and I am sure you guys know why it has to be done by someone who is not tainted by the internal politics attached to certain views regarding the organization. So we do that facilitated process.

But in the facilitated process will it be all divisions or would it have one for operations?

It is everyone, so the entire organization – which is a good thing because the organization, despite the fact that we are compartmentalized when we want to structure

our work, that work is cross cutting in certain circumstances; some people may need things from me in order to do their own work and may need things from other people to do their own work. So it is important that you should have everybody under one roof.

Okay. Question 10: Does risk management form part of any KPIs or even job profiles at any level of the organization? I want to know at what level do people have in their KPIs, a KPI that looks to risk management?

Oh you mean in our performance agreements as managers?

Yes.

Yes we do, but again I don't know whether that applies across the organization. Ja, we do.

Say for instance for a person at your level you will have something.

Ja. I do. It is part generally of a … what is it… it would be part of a broader KPI for a manager, called leading and directing your unit: so when you lead and direct that unit you must manage risk as well, within your unit. So it is one of the KPIs.

But it doesn't clearly stand out to say Risk Management, it is just part of the … or is it..

It is a KPI, but I am saying like you have a key performance area and that says 'please make sure that you are managing this unit of yours and directing it properly' and then under that they will have a key performance indicator that says 'manage risk' and then you have a key performance indicator that says 'manage people' and you know..

Alright, that is fine. No 11: Here I want to understand allocation of resources. So these resources can be human, can be other, any kind of resources.

Financial..

Ja.

Technological.

Ja. So I want to know how this risk management system influences the allocation of any resource that has to be allocated?

You want it here at SAWS?

Yes.

No, it doesn't really influence it but…

It doesn't?

No, unfortunately not.

So if you allocate your resources what do you base them on?

Just base them on the work, in fact this is the planning process, that says define your work and allocate resources. And then define the risks. I don't think directly we do that. Again, I am talking for myself, I don't think we have a direct way of doing it, what we try to do is to say that for instance for financial resources, if you are saying you are going to do this amount of work do you have budget to do it?

So that..

Therefore in that case if you have so much budget don't say you are going to do so much work because you are obviously not going to be able to do it if the amount of money doesn't allow you. You should be doing the same with people resources, but you must remember the people resources tend to be very static in terms of their allocation, have a certain structure. You don't then say okay, I am going to increase my amount of work this side and because I had so many number of people doing service in this smaller amount of work, at the moment it is increased then I will increase the people resources – which indirectly is an increase of the finance part because you have to pay those people. Ja, it becomes difficult to do it that way because of budget constraints from the money we get. Ja, I don't think we do it directly; it is an indirect thing.

Okay, so maybe indirectly but then one way or another there is some link as to how resources are allocated to the risks that are identified.

It would be a very loosely defined linkage. It's defined in the same sense that I said that everything at the end of the day is linked to your strategy planning, but you don't have a solid link that says that 'let's look at those risks and then think about the budget that we have'. We look at the risks and say that when for instance we determine why we would not achieve, or what would be needed to mitigate against the risk you could then say 'ah, you would need funds'. Now you need more resources. But what you then don't do is to then say because that risk says or is about more funds or more people,

new technology, you don't then go and develop that new technology or employ more people, because the people who give you the money are not the same people as the people who run the organization. That is the first thing. They may not see the importance of what you are saying. In fact they don't even look at these things.

Right.

But ja, again it is one of the things that theoretically it should be done that way but you look at the type of organization that you are at, and it is not done that way.

Okay, that is fine. Last question, no. 12

The most important one.

Here I wrote and wrote and tried to explain it, but I think it would be easier if I just explain it to you.

Sure

Because it has two legs, because I am imagining say for instance there is your organization here in the middle. Now this organization needs to abide by some laws, international laws and all sorts, so they need to be able to comply with those rules. And at the same time I also think that there might be other regulations that are created by your organization itself for other people to abide by – maybe some of its stakeholders. So I want to understand if the risk management system is it able to influence some of these compliance levels? Like does it help to make you compliant to your own …, or will it also help you make sure that the people that you want to comply by your rules, do comply also.

Ja, in the ops division risk profile or risk matrix there is a lot of stuff that has to do with complying with international obligations. So a lot of the risks there are linked to that. In fact there is also a risk that is related to business continuity and within business continuity again, you also take this risk matrix and align it with business continuity and now business continuity has a direct linkage to this complying in the first instance because it says we always need to have this kind of information by this time at all times, so if your business is affected one way or another by some disaster, then you must make sure that this and that is catered for. So that also forms part of our risk, or the input that goes into the risk matrix. In fact if there is one area where there is a very

direct and strong linkage, it would be between our business continuity planning and strategy and the risk, certainly within our division of operations.

So now in short yes, the risk endeavors here help to make sure that compliance levels are maximized.

Yes. I think again it is done, it is happening because of the whole cycle of planning that exists. I am not sure whether someone sat and said 'ah, you have got risk management here and you have got business continuity, and you have got strategy planning and we have got things to comply with, then let's make sure that the whole process is synched'. So I don't think we have got such a thing, I think it is just a consequence of these things being related in any case. But there is a strong linkage between the risk management and business continuity.

Okay, I think we have completed the questions, I am going to switch off the recorder.

ENDS.

9.8 2013-08-22-11h00 Interview

Like I explained, there is no wrong or right answer, so all the answers you give to me, remember will be used in aggregation, with the aim of creating theory, so my research is qualitative and so I have read a lot of theories and articles and I just want to see what the people that deals with these things in the public sector says – as opposed to what the theory is saying and then at the end I will try and create my own theory based on what I understand from your answers. But there is not going to be something like Buta said this, Mark said that – it is just going to be an aggregated response at the end. So don't worry at all about confidentiality, absolutely you are protected.

Okay, so I am going to start with the first question, it is three things in one for question one I realized, so maybe it is easier when I break it down, but if you want to answer it all at the go it is still fine, because I want to understand from you here at the Weather Services, what forms the basis of risk identification, like if there are risks identified, where will I get that, what is the basis of that whole methodology or system or whatever you use to base your risks on?

Okay, well first I mean I have been working on risks now for some time, okay not purely on risk but involved in risk management initiatives. So the very first basis will be King III requirement, that management should identify risk and ensure the mitigation to reduce exposure to the shareholder and also to the organization. And internally, on a practical level, we need institutional knowledge, people with institutional knowledge, who understand the processes, understand the procedures and the day to day things that are going on with the organization, to actually be the people who can contribute to identifying the risks that are there, okay, and then also to contribute to the mitigation, the mitigation plans, okay?

Ja.

There is usually a risk framework that is used, okay? So you follow that, and then … ja. But the basis and really the need is driven from the governance requirement as well as

King III and the PFMA

And the PFMA, ja, but to actually identify you need people who understand the business, you know, people who are involved with day to day work so that they can be able to pinpoint these are the areas, these are the weak points

Down in operations you mean, or at a strategic level?

You need.. your management, because there are two classifications of risk, you have the strategic risk and the operational risk. Yes. But even at strategic risks, you have to cascade them down to operational level.

Okay, so we are talking about the basis of the risk identification, so the assessment also I guess.

Yes, it's there.

It will also be made at that level, whether it is strategic or operational. And then the mitigation plans for it.

Then you will have your risk register and all that contribute to the framework that you are using, you know, that is assigned to the risk owners and to do risk rating and risk profiling and blah blah blah.

That is exactly what I want to talk about actually, now that you bring it up – the risk register – because I imagine there would be a risk register from operations, from the operational level and at that level they will identify their own risks and do the assessments and come up with their own mitigation plans.

That's right.

I want to understand how that risk gets escalated and captured when you do your strategic objectives, or at the strategic level.

Actually it is the other way round: it is first the formation of strategy.

Objectives

The strategic objectives, and then the risk identified at a strategic level, and that obviously then has to move down, cascade to operational level, because operations must in a way, the operational risks must address the strategic risks, yes, they must address them, otherwise there is no coherent seamless flow of activities. Okay. So it goes from that level down. Obviously at an operational level the risk register will be more detailed, there will be more details and there will be…. I mean that is why some of the information it is not strategic, you have to operationalize it, so then you find that when you have maybe four or five risks at strategic level, at operations there will be so many.

Yes. Now just clarify this one for me, so you are saying you are talking on the top down.

The top down.

Only. Because I want to now understand… I understand fully that there will be those that are top down because the objectives of the organization is made from the top.

Yes.

And then like you said correctly, based on those objectives then you will come up with the risks, because the risks have to be in context of what the objectives are.

That's true.

Because we will never have just risk coming from nowhere.

Hm.

So now that we have those objectives first and then the risks based on the objectives, then you are talking about the top down, to say 'okay, this is what we think are the risks' – and cascade them downwards. So I want to also understand, what about the emerging ones, that comes up, I want to find where the linkage is, or…

Ja, I mean operations develop their own risk registers which are done at a divisional level and even at a developmental level to inform the divisional risk division; that is where you will have emerging, new risks that are being identified as business happens, because while you are planning, life is happening. (laughs) Okay? And those are captured you know, in what one would call emerging risks, depending on their priority, and they may be addressed immediately or they may..

..remain at operational level

You know, leave them at that level and then put mitigation plans for them. And eventually incorporate them to inherent risk, you know? And even though I said it is strategy that informs operations, but remember to inform that strategy, there is operational information that goes in, you definitely have to do your situational analysis, and that's why you are looking at your internal environment as well as external

environment, and in your analysis of the internal environment, you will have to address all the things, that is where all those known issues in the organization, business, are factored in, and in doing our SWOT analysis, these are our strengths, these are our weaknesses, blah blah, and you do your Pastels and so on. So operations will inform strategy in a way, but then it slows down.

Okay. So we have done one, and I think in a way we have also integrated no 2

How organizational risk is integrated and encompassed into formulation of strategy – ja, we have.

Hm, because although we have talked about it but I also just want to confirm, just for clarity purposes, to say okay, I am asking you how are the organizational risks integrated and encompassed into the formulation of the strategic objectives. So let me just confirm, you did say that the strategic objectives are formulated and based on that then the risks can be formulated to say based on these objectives these are the risks, and those risks will take into account the operational risks?

Ja, the operational risks will also inform strategy you see, because what is strategy? You know in the Chinese language it is out of walk, it is how the organization positions itself to deal with business challenges and the landscape where the business is operating, to be viable and relevant. So the risks that are there in that landscape do inform strategy as well, that is why you have to do your Pastel, look at the political landscape, the economic landscape, what risks are there and how does an organization, what strategy should an organization adopt to better position itself in that landscape. So yep.

Okay, so we are saying there are core parents, so they are intertwined.

They are intertwined

You will look at them in the same breath as you will be wanting to be set up your objectives, but you also have to look at operational issues.

Exactly.

Okay. I am happy with that. So these operational plans will also be based on …whatever operational risks, will be based on the strategic risks.

Yes.

So that is fine

Operational plans is what you cascade down to say how do we then implement the pie in the sky.

The strategies Ja. No, I get that. No 3: in your own understanding, how significant is this whole risk thing in your organization.

How significant is our risk concept?

Ja, when they are formulating the strategy or the strategic objectives?

It is very important, very, very important. Even at here we don't have unlimited resources, there is human resources, even financial resources, I mean we operate within those constraints and by their nature they pose a risk in what we must deliver as per our mandate – this is the capability we have.

What is available.

Ja, what is available. So the concept of risk is in the core, it is in the core of how do we survive, how do we remain viable and relevant you know?

Okay. I get that. How does the organization know how much, like how does your organization know how much risk it is willing to take? So I want to understand the risk tolerance or the risk appetite policy if you have one, or whether it is written or unwritten because you know some of the things happen even if there is no official, formal document. But what is the understanding among management as to what is the risk tolerance, what is that based on?

Look, I think the first answer will be that the board will determine the appetite, the risk appetite of the organization, because they are the custodians of the risk. So management may not do that, it is decided by the board you see. Yes, I mean there may be areas where we have a resilience, a risk resilience, in certain areas where it is really not substantial, you know, because understand that your risk appetite is related to the amount of money you are willing to forego to gain an opportunity in a business or the gains assess your loss! Ja.

But at the moment, I think at this stage after doing a few interviews at here I do have the sense of the risk maturity if I can put it that way. Where I am employed, I

am sure you have seen my emails and I have also done a few years, I have just been doing that. So also because I think my company is also much bigger when I compare to yours, yes, there will be separate risk appetite and tolerance documents that the management is clear on, as to when we say this. So here, even if it is not a separate document yet, but if you had to interpret your understanding of it, you would just say that as far as you understand there is a big appetite or not really – to take a risk here?

(laughs) This is… I cannot speak on behalf of my organization.

Yes, I know.

But my own opinion, we really are stressed in terms of the resources we have and the mandate, we are initializing government support, but there is more demand for us to actually generate ..

Your own revenue

Our own commercial revenue to balance what we are not getting from government so there are competing needs and limited resources. So I would say our appetite will not be that huge.

But would you not then say that seeing that you want to maximize whatever revenue you can get from wherever, and that is an opportunity for you to take even more risk, or not really? Because I would imagine the more risk you take the ..

The more (laughter)

Because if you want to get more revenue you take some, give some somewhere – give and take.

No I think people like Resilfo would be in a better position to answer that one! (laughs)

Okay. Alright. There is appetite, but you really don't want to be pressed on a corner. That's fine. No. 5: so here I know you can never really know, but there should be some stage when you are formulating strategy based on what you know now, say based on all the information that we have now, can we really get to a point where we can say that at this stage we have covered all the possibilities we can think of and so at this stage we are comfortable that all the

bases are covered? Or do you say it is not possible that an organization can get to that stage?

Before finalizing strategy, which we do, I mean there is a five year strategy and we do annual reviews, and then we do annual reviews for the very fact that you know we are living in a dynamic environment, things are forever changing. Strategy that we set a year ago, five years later you know your environment will have changed, political environment is changing, economic environment, you know dollar to rand exchange, that is forever cycling. So there are uncertainties, so strategy is drawn in casting your eyes to the future; we are taking into account there is a degree of uncertainty to what the future will look like, but we base our decisions on what we know. Now, what we can see, and the level of predictability that we as a collective – because remember strategy is not one person – so it is a collective input. So as a collective we say we are comfortable that at this moment we have this level of predictability in the foreseeable future, this is what we are confident to document and put pen on paper to say this is how we proceed for now, in the foreseeable future. But eventually, every year we do have to review, that is why we do our reviews. So yes, at a point of rolling out a strategy, we do say we have a strategy, we are confident it is a document that we as a collective have come up with, we are confident it is workable, the objectives are smart, you know, they are measurable, and then we work on that, but as in the next year…

Things change.

And sometimes in the annual review there is not much that has changed, and we say not much has changed, we leave it like that. Okay. But there are cases where you will say something that you did not see coming has happened and you know so much needs to be adjusted and modified. So there are no total re-writes of the document, we are seeking to say are there gaps, did we miss something. So there is certainty but there is also uncertainty.

So you are saying that at a point in time we can say based on what we know now …

..we are happy with what we are seeing. Yes.

Okay, the annual strategy reviews, annually you will look at the total strategy and you will want to see based on the external and internal environment what is going on. Now before that strategic review comes, in between, you revise what? The risk registers themselves?

The risk or risk register, we also have to review.

When, in the annual sitting or.

No, there is a different forum for that.

Oh.

Yes, there is a case where there is a risk management committee, which comprised now mostly of the senior managers and some executives – mostly. Actually all the EXCO members are there. And some of the senior managers. And then we sit as a risk management committee and review our risk register. Okay? And divisions also have to review their operational risk registers. Okay? And to see that the mitigation plans or the treatment plans for the risks that are there are valid, they are still relevant and also because some of the risks may not be treated in the same year, so you want to see also the progress.

Okay. No 6: Can the risk profile change after formulation and during execution? What happens in that instance? Maybe this is more like what we were saying, that…

This profile change after formulation and during execution? Well I mean I think one thing to be mindful of is the risk register, because the risk profile is almost a final product of the risk formulation, you see the risk register is formulated based on knowledge of the inherent risks within the organization and the business, so the changes, it is unlikely, it is unlikely that it will drastically change because it is what people know, it is what has been happening, the risks are the past, the present and also like we say what is in the future – that goes into that. Okay? So after that risk register has been collated, it is there and then we profile it, we rate the risks and profile them, and obviously during the course of time the risk profile may change because there will be certain control measures, and they may reduce either the impact or the likelihood of the risk and then that brings adjustment to the final rating of the particular risk and that will mean that maybe where it was a high risk it will maybe go to medium or even low risk, you know, and it even may get to a point where we feel that this risk is no longer a risk. So yes, if you are looking at after control measures have been implemented and the risk has been treated, the profile will eventually change. In fact the whole point is for that profile to change, you want it to change, because we must treat that risk, it must not remain the same level.

Month after month.

If we keep seeing the same risk year after year ..

Someone is not managing

We are not managing, we are not even implementing our plans, our mitigation strategies.

Happiness. So no 7: Also I think we have done this. How often can or is the review of the organizational strategies performed, aligned with ever changing internal risks?

Definitely, yearly.

Yearly. So whether they are there also in a written form or not, what are the specific steps involved during the review of strategies? Are there steps?

Look if you say steps, do you mean a standard procedure, or… There is with strategy planning, there is a structured approach; it is always a structured approach where you will begin with what exists, you know you look at the mandate, the organization, us as a government entity, you look at our mandate, has our mandate changed, you know, and the vision, the mission.

So are those things done on annual review?

These we always do them all the time, every year, because you remember things change. I mean we may have a new minister, maybe a new president, but a new minister and we may no longer be an entity of (laughter) So we have to look at all those things, most of the time certain things remain constant, they don't change, so you must know that this is still the same and we are still happy with the way we have defined it, we have phrased our mission and our vision. Is there a change in that? If we are still happy then we are happy. We move forward. So it is a structured flow of activities, how you treat the strategic review.

Does it happen over days or…

Usually about three days.

So it will be a review of all those missions and everything.

We review the vision, the mandate, the mission, then you go to your strategic goals or objectives, and eventually you have your frame where your strategy goes, your strategic objectives, and then you put in the key performance indicators to measure them, and time frames and all of that will be in there. I don't know if I am making it clear

Yes, I think it is clear enough.

Ja, it is very structured, it is very structured, otherwise we will spend the whole week and not come out with a product so it is also usually facilitated by an objective external facilitator who will not get lost in detail like us internally, where we start debating issues internally. So the facilitator is there to make sure we have followed the structure

Okay, I get that. No 9: what is the significance and evidence of the risks during the review? So say there is a structured way things are done like you said, over a three day period to review, I want to understand, because if I want to come in and say okay you have done your strategic review, you look at your risks and you did everything and now you are happy – what is the evidence, what will show that risk whatever, whether management or methodology or just risk, what evidence would be there to show that the risk issues have been taken into account?

How will you know that you have taken the risk into account during the strategy session

Yes.

I think one of the initial pages of the strategy document, you also usually find the strategic risks that are listed there, because we have gone through them, because they are guiding principles as well; they form part of the guiding principles to the strategy.

So there will be that strategic document.

Ja there is a strategic document and in the first few pages you will find there are guiding principles and one of them will be the strategic risk that the business has taken into account.

So you have been to the three day workshop, there is a strategic document that will lay out the strategic risks, so what will show that those risks were ..

The strategy does address, I said the strategy informs risk, but it is actually the other way around, the risk informs the strategy.

Ja.

You know?

What comes first? You said the objectives come first?

The strategic objectives is not first. You have got your risk, your strategic risk which are part of your situational analysis as well, because as you are doing all of those pastels and you also have to look at what risk does the organization have, and you know, and are these risks still relevant and you have to address that. And all those then, plus your internal constraints or your internal environment as well, will inform your strategy in terms of you will then say this is now our strategic goals or strategic objectives. So strategic objectives are in the bottom.

So they are formulated after looking through everything else.

Everything else. You have to scan your environment and (laughter)

Because I am sure at first you said it the other way round.

Did I say it the other way round?

But it's fine.

Okay.

Okay, so now I get that also. So we are saying that the evidence will be the fact that…

You should see a flow in your strategic document, a flow which indicates that what you have identified as strategic risks is in one way or another addressed in your strategic objectives and in the way that you implement the strategy.

Okay

Because that is what the strategy is about, it means positioning the organization to deal with the threats, deal with the challenges, which affect the organization.

But most importantly, because most people just look at the threats, but also to take advantage of the opportunities.

That's true. Even the threats you can turn them to opportunities.

Yes.

It depends which way you look at them.

Yes. Because most of these risks that we put in the risk registers, in fact all of them, if you feed them around there is always an opportunity.

Yes, in fact late last year when we reviewed our risk register we learnt that even the way that we phrase risk, now we have to phrase it in a positive way. You know we used to have negative risks, negative is 'lack of' 'failure to' you know, and..

I know at my employment also, for years we were in that trend but now we… Okay, so we are on no 10.

Yep, we are getting there.

Does risk management form part of any key performance indicators? So I want to understand from which level would the risk, specifically risk management, be part of the KPIs? Or even your job profile, you know your job description, to say what you are responsible for.

Ja, okay, well the answer may not really be very clear but the way our performance management system is applied in the organization is such that we try to reflect in the performance agreements, the key imperatives you know, of the division, because they are done divisionally and cascaded down. So from the development manager, his/her performance agreement must address the organizational imperatives, which are enshrined in the strategy and some of them in the risk register as well. Okay. And the people that report to that head of the division, their performance agreements must talk to also to the deliverables of their head, to support the implementation of whatever is in his/her performance agreement – which actually is talking directly to the strategy and the risk register. Then it comes to operational risk, some risk may not be linked directly to the operational divisional head, it may be linked to people below him because they are operational by nature you see. So yes our drive all the time is to tie into the performance management agreements, the important key performance areas. And how do we measure performance? It is not performance of individuals, ultimately the collective performance of individuals must translate to the performance of the organization and that is how our performance management system is structured. So individuals perform, and it must show in the performance of the organization.

It could influence the whole..

Ultimately. So you cannot have a situation where performance of agreements of individuals are just going on their own, off on a tangent, not aligned to the

organizational goals and objectives and they are not addressing the risks which we know are there.

So in other words not at all levels there will be a clear thing that talks to risk management but the major activities that need to be performed are part of managing the risks all the way.

That is how we look at it. There are some risks, I mean every risk has an owner, there is a risk owner.

There should be, and the due dates.

Ja, and there are those due dates by when, and what are the activities around it, and when are those activities deliverable. So for some risk owners you may find that some risks are directly, can even be taken verbatim into their performance agreement you know? But in some cases they are implied in performance agreement, and being supported maybe by some people who are supporting that line function.

Ja. Okay, happiness. No 11: How exactly does the risk management system affect the allocation of resources, being of human or non-human nature? So in other words whether the resources are electronic, technological, the IT things, or financial resources, human resources, whatever, the physical security issues – when you allocate all of these things do you look into the risk implications, or how does the risk management system help you in allocating?

Well I think I can say what drives our activities is operational requirements, actually they are not literally driven by risk per se, but by operational requirements. So operations is what we do.

So it will dictate which resources must go where

Yes, that is what it will dictate, in fact you will find most of our resources are allocated to operational imperatives, you know, where we must deliver a service or a product to a client or for public good or whatever, and the resources that are allocated to that, obviously there will be certain risk that ties around that activity, but the risks are not usually the drivers; it is the operations that is resourced.

Ja, but do you find that maybe based on that, do you find that if you take most of the resources to the imperative activities then also the imperative risks will also lie in there, or not really?

Most of them are there, because where do you find most of your risks? You find it where there is a concentration of your activities (laughs) you know? That is where you find most risk as well, and there are financial risks because of the amount of financial activities you are having, and the procurement we are doing, and there are risks related to that and in IT, we are an IT intensive organization and there are certain areas of IT risks that we have. So the operations are trite, certain risks on their own, so even if you look at the distribution of our risks you will see that they are concentrated around areas of high activity. So ja, you will find that even though you may say we are not resourcing the risk, risk is resourced indirectly.

Risk will just follow where things are happening.

Yes. Ja

Okay. The way you put it is 100% but I just wasn't thinking about it in that particular order but absolutely it is true. So the last one, this one I must just explain it because the way I have put it here is a bit confusing. What I want to ask here is say for instance the this organization which needs to comply to certain regulations, so your organization needs to comply with certain International regulations that you are hounded by, and at the same time my thinking is that also you as an organization would also create some policies and what not that you want other stakeholders to comply by. So in other words you need to comply by other rules by someone, and someone else needs to comply by your rules, whoever your customers are. So in that instance, how does the risk management impact on your compliance levels, whether you have to comply with international rules or whether some other international or local customers needs to comply by your rules? Is it affecting the risk management or not really? Does it help you comply or…

Look one of our strategic objectives talks about compliance to international and national legislation and regulation, you know? It is right on top, the strategic level, and I mean that gets translated in various divisions depending on what regulations are affected. So if you talk about compliance it is all over; we all have to comply one way or another to some legislation or some regulation or some regulatory requirement. So yes definitely, because we are a global player we are involved with all world related organizations, the ICAO, the International Civil Aviation Authority as well, so by the nature of what we are doing we have to comply, and our products we produce have to comply to those standards. We are in a very sensitive industry which is aviation, we

have to supply a particular product in a way that it is packaged and of a quality that they require. So yes, we have got those demands placed on us. And like I say because it is so important, these are things that define whether we survive or not, and also we don't have, I won't say we have our own regulations..

Don't you have some that you expect other people to…

No, I won't say it is ours, we do extend certain requirements to our customers or clients, and we extend them like national treasury regulations for instance, PFMA, you know? We will extend them to our service providers.

Okay. So are you saying..

The triple BEEE, all those we extend them, so we have to play within the ambit of while we are complying, but we also expect compliance.

Because I want to understand, I am sure public sector institutions in the past five years or so, have had to really focus on risk management as an official phase, because usually there wasn't anything like that before. So now I want to understand that now that more and more public sector institutions including your organization, mine and all of them are trying now to get into the habit of now keeping the risks .. and actively managing the risks, does that help with the compliance levels? Would you say that this practice of these committees and risk registers and risk this and that, helps in the compliance levels, or you were going to comply anyway whether or not there was a risk management system?

Well I mean for the risk management thing, okay there is two sides to it: you say there is compliance, definitely, but we don't do things for the sake of compliance.

I understand that, yes

We also do them as a matter of good practice.

I hope so, yes.

Ja, as good management practice and good governance. So for us the risk management methodology works also for governance, also as a management tool, because it gives us a structure and a way of following through on our matters to the end, so things are not left hanging and then they fall within the cracks and then they pop up one day and you know it becomes a huge threat to the organization. So it is

both for governance, for the management tool – yes. And compliance! Maybe compliance is not even the first thing.

Ja, it is just a by-product of good management and practice.

Yes, and eventually compliance. But if we did it only for compliance we will not do it wholeheartedly.

100%

We have TQM as well as we are an ISO certified organization, this is our own initiative as an organization that we took the trouble of starting this process, this journey, to get to be certified as a service provider to our clients, and also as a supplier to those who use our product. And to some people they say TQM is a lot of work but we have said it must be enshrined in the way we do our daily activities, enshrined in the way we do our work. So it becomes part of life, part of the way we work, as well as a management tool as well, that someone else can say TQM is for compliance, because some customers will require TQM. Obviously WMO, to which we are a member, requires and even ICAO states that members of this services will be quality certified. But you know that we have been the first ones, the first ones, to have this.

First ones in..

In the region, in Africa. We were the first ones to do it and it was not done for compliance, it was done for good governance, but it is already serving, it is taking into account compliance as well. So what I am trying to avoid is to say we do risk for compliance reasons.

So you are saying that risk management is done as part of the system, the compliance levels will increase due to the normal management activities.

Definitely because we are reducing our exposure levels to unnecessary faults and failures because we are taking care of the risk that are inherent, we are reducing risk from inherent to residual risk and eventually to no risk. And so we are always manage to obtain unqualified audits when other organizations are getting qualified audits and we ask why – it is because of the way we work.

Is your organization a member of SAQI, that is South African Quality Institution?

SAQIS? We are hosting SAQIS here.

Is it?

We are actually the hosts of SAQIS

Okay. But because I know a while ago at my employment we registered us and I do get this quality monthly magazine from SAQI

Okay.

So this organization is also a member?

You are talking about the equality…

No man, the South African Quality Institute?

Oh, we are talking about different things, I thought you were talking about the equality.

No, not the equality. That is your business, your people. Okay I think I am going to switch it off now. In terms of questions I think we are done.

Okay.

ENDS.