Investigating challenges related to the successful implementation of risk management processes: A South African risk practitioner perspective

DA van der Merwe

orcid.org/0000-0001-9449-6788

Mini-dissertation submitted in partial fulfilment of the requirements for the degree *Master of Business Administration* at the North-West University

Supervisor: Prof I Nel

Graduation ceremony: July 2019

Student number: 28328957

ABSTRACT

Risks and risk management are part of our daily lives, whether in the work environment or in our personal lives. Decisions such as whether or not security guards are required, or whether or not to advance credit to a potential new customer are examples of risk management. The term risk management is a more fitting term than the terms risk removal or risk eradication, since there is a strong relationship between risk and reward. Lower appetite for risk will more likely than not result in lower rewards..

Financial service entities provide essential services to the public, such as providing the means that allow for banking to take place, or providing financial protection products such has insurance.

Financial service entities such as banks face numerous risks, both internal and external. These risks range from strategic risks such as competitiveness and innovation, to the more operational risks such as processing errors and theft. Industry loss statistics, scandals, and risk experience suggest that financial services entities may be experiencing problems in successfully implementing risk management.

The objective of this study was to determine the most pertinent barriers to the successful implementation of risk management, specifically in financial service entities. In this regard, failure has a broad meaning: from not realising the true potential of risk management, to an entity collapsing. In order to determine these barriers, 24 interviews were conducted with risk practitioners – a suitable group because of their first-hand experience and knowledge of the challenges related to the successful implementation of risk management.

Questions posed were primarily developed using the findings of existing literature on risk management, as well as literature that dealt with project implementation, in order to crystallise implementation-specific challenges that may be relevant.

This study highlighted critical barriers previously identified by other researchers, as well as certain barriers which may not have been considered as serious until now. The following four key themes arose from the research, and reveal the most pertinent barriers to implementing risk management successfully:

1. inadequate buy-in from operations;
2. no risk appetite is defined; and
3. risk practitioners have insufficient knowledge of the operations.

There are three key findings from the study. The first is a practical take-away from the study, namely that senior management should conduct cultural interventions that advocate for the importance of risk management to improve buy-in. Second, the importance of having a risk appetite stems from being able to determine the amount of controls and effort to expend in managing risks – this balance can only be determined and achieved if it is clear how much risk is acceptable. Risk management is essentially maintaining the desired balance between risk and reward; this is embodied by a risk appetite. Last, for risk practitioners to be able to contribute meaningfully to the risk management programme, they must have sufficient knowledge and insight of the entity for which they facilitate risk management.

Keywords

Risk, risk management, objectives, uncertainty, benefits, barriers, risk appetite, financial services, controls, risk practitioner

ACKNOWLEDGEMENTS

Through mercy and grace alone have I been able to reach this point, and I am forever grateful to God.

Thank you to my parents, Abraham Lodewyk and Miemie van der Merwe, for always being there for me no matter what, and for always supporting my studies. To my sister – and professor in the making – Leoni: words cannot describe how much I appreciate you for being a true friend and role model.

To my supervisor, Prof Ines Nel, I would like to say a huge thank you, and acknowledge your patience and understanding throughout this process. It was an honour and a valuable learning experience that was worth the time invested.

Thank you to the individuals who took time out of their busy schedules to provide valuable input for this study. I trust that we will slowly but surely improve the risk management discipline.

A general thank you to all the lecturers and support staff at the Business School, and a special mention to my MBA group, Unity Group. It was tough but fun.

Thank you to each and every person who supported this endeavour in any way.

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

LIST OF ACRONYMS

AIRM	Association of Insurance and Risk Managers
ASA	Accountancy South Africa
CAANZ	Chartered Accountants Australia and New Zealand
COSO	Committee of Sponsoring Organisations of the Treadway Commission
CIMA	Chartered Institute of Management Accountants
ERM	Enterprise Risk Management
FSB	Financial Services Board
FSCA	Financial Sector Conduct Authority
IIA	Institute of Internal Auditors
ISO	International Organization for Standardization
SABS	South African Bureau of Standards
SARB	South African Reserve Bank

CHAPTER 1: NATURE AND SCOPE OF THE STUDY

1.1. Introduction

Risk management is intended to ensure that an entity (whether for profit or not) is aware of the risks it faces, and decides on the relevant treatment options so that it achieves the objectives it has established. Risk management is increasingly becoming a priority (with the allocation of resources). In addition, certain barriers should be removed or navigated to realise value from risk management. The first step in this process is identifying what these barriers are. This study is premised on the opinion that risk practitioners are best placed to provide input for this subject, since they likely experience or observe such barriers.

Risk management and corporate governance have been buzzwords for many years, and are not losing their relevance – it is more likely that the demand for risk management will increase as uncertainty and complexity increases. It is therefore prudent that efforts be made to realise the potential of risk management, rather than merely going through the motions (Waterhouse, 2015).

Due to major risk events that have materialised in recent years, as well as a notable drive from regulators, increasing attention is being devoted to the concept of risk management. This leads to increased resource allocation to enable risk management in the form of human capital, systems, processes, and structures. Thus, risk management and its implementation present a number of costs to the business in the form of staff costs, time costs, costs related to risk structures, reporting costs, and (in certain instances) software costs. Surely, this cannot be done without some sort of return on investment.

This study aims to determine the most pertinent and common factors that prevent risk management from enabling the achievement of objectives, in such a way that solutions may be implemented to reduce wasted investment. The study made use of interviews to obtain qualitative data from risk practitioners in different entities to ensure that a representative response set was obtained.

1.2. Background

Increased competition due to globalisation has introduced not only more risks, but new risks. Coupled with the increased dynamism of technological change, this has resulted in higher levels of uncertainty, and it is this uncertainty that drives risk. Simply put, risk is defined as the effect of uncertainty on objective realisation (ISO, 2018). Managing risks, whether in a structured or unstructured format, has to do with ensuring that the organisation realises its objectives.

The benefits of risk management are not always visible, especially if there is no possibility to compare them against a base. However, there are two specific examples where the benefits are obvious. First, the benefit that banks realise in the form of having to hold or reserve less capital under the Basel (Bank for International Settlements, 2018) and Central Bank provisions as a result of mature risk management in the respective banks. Second, the benefit that individuals and corporations realise in the form of more favourable credit terms (pricing and restrictions) due to managing their credit risks better.

Christopher Palm, chief risk advisor of the Institute of Risk Management South Africa (IRMSA) makes the following observation with regard to risk management in the 2018 IRMSA risk report (2018:9):

> If risk management is properly embedded within an organisation and a strong risk culture adopted, we will see more organisations being able to maintain stability during times of difficulty and seize the 'opportunities' that come their way to prosper. One may therefore argue that the implementation of an effective risk management programme may increase the probability that the responses to risks would be more efficient and effective.

In the literature and the various standards supporting risk management, risk management is presented as a business enabler that either creates or protects value. Therefore, it is important that the potential value it is supposed to generate is realised. A 2008 study on enterprise risk management (ERM) as a business enabler within the City of Johannesburg Metro found that the municipality failed to achieve its objectives due to enterprise risk management not being implemented and driven adequately (Makoro & Van der Linde, 2008). This is yet another endorsement of the importance of risk management within the South African context that provides the motivation for

conducting this study. Actions taken within organisations, specifically those with profit objectives, should bear some sort of return on investment.

In a study undertaken by Pillay and Zaaiman (2015:3) on risk management within a South African municipality, buy-in for the importance of ERM was identified as the key problem in implementing risk management. The study further identifies the factors driving the lack of buy-in, and potential enhancements to get buy-in to an acceptable level. The three most pervasive factors were first, poor high-level corporate sponsorship for ERM; second, no integration of ERM into strategic planning or processes; and third, inadequate capacity to manage risks. The results of this study are significant, because if buy-in is not achieved, it may render the entire risk management effort worthless, since it can be regarded as one of the initiators of any change effort. If there is no buy-in, it is likely that the effort made to implement ERM processes will be poor, or no effort will be made at all.

South Africa has a number of sectors where risk management is a mandatory function that must be in place, such as banking, insurance, and even in the public sector, in the form of legislation, such as the Public Finance Management Act (Act no. 1 of 1999). Governance standards, such as King IV (Institute of Directors Southern Africa, 2016), note extensive risk management requirements that entities listed on the Johannesburg Stock Exchange (JSE) must apply. In this instance, risk management is primarily focused on the sustainability of the entities, which translates into the protection of the shareholders' investments in these firms.

The management of risk is now, more than ever, a critical strategic enabler that must be undertaken as efficiently and effectively as possible if organisations are to prosper; barriers to realising the benefits of risk management must be identified and minimised.

The primary aim of this study is to assist risk practitioners (and, by inference, their respective organisations) to be aware of the challenges that they will face in order to embed risk management, with the aim that this awareness better prepares risk practitioners to mitigate the identified barriers, thereby realising the benefits of successful risk management.

1.3. Problem statement

The key research problem for this study stems from the fact that while risk management theory, structures, and resources may be taken into account (at a cost), the benefits are not always realised, and can thus be seen as a wasted investment. This has been outlined in the background section in terms of major incidents and scandals that have occurred in recent years in entities where risk management exists.

This study aims to determine the causes of poor risk management performance by identifying the key barriers for risk management implementation.

1.4. Research objectives

1.4.1. Primary objectives

The primary research objective is to determine the most pervasive barriers that prevent risk management from delivering intended results from the viewpoint of risk management practitioners.

1.4.2. Secondary objectives

Objectives for the literature review

Studies that provide insight into the reasons why risk management implementation is unsuccessful were consulted.

Empirical objectives

Interviews with risk practitioners were conducted to determine which factors impede the successful implementation of risk management. These interviews will take the following factors into account:

- personnel factors;
- organisational culture;
- economic factors; and
- factors related to skills, knowledge, and training.

1.5. Research methodology

The research methodology sets out the techniques employed to gather data that will be processed into information at a later stage (Burns, 2008). It outlines the approach that the researcher followed to obtain the necessary information to achieve the research objectives.

The research intends to explore the most prevalent reasons why risk management does not deliver the desired results, as experienced by risk practitioners.

1.5.1. Literature review

The literature review presents an in-depth scrutiny of past studies related to the research topic, in order to identify key findings that helped to answer the primary research question. This entailed consulting sources such as journal articles, dissertations, and other investigative reports that address topics related to the successful implementation of risk management.

The secondary data used to answer the primary research question predominantly focused on risk management in South Africa. Previous studies undertaken by Pillay and Zaaiman (2015), Makoro and Van der Linde (2008), and others were reviewed. Publications from electronic databases, as well as libraries, were used to complete the literature review.

1.5.2. Empirical study

1.5.2.1. Research design

The research will be qualitative in nature, according to the guidance provided by Leedy (2010:106), which lists the following criteria as good proponents for qualitative research:

- multiple possible realities;
- the research question is exploratory or interpretive in nature;
- no hypotheses or cause-and-effect relationships are to be proven; and
- a relatively small sample will be used.

The research type is a descriptive study, as it intends to gain insight into the subject, and establish answers to who, what, why, and how questions. It builds on exploratory studies previously conducted on risk management. The research was conducted with the view that it would not necessarily produce conclusive results for decision making, but would yield more information on the subjects of risk management and effective management, in such a way that certain courses of action can be decided upon (Lambert, 2012). Lambert (2012) further suggests that descriptive research is well suited to studies where the intention is to explore straightforward phenomena, and for presenting the results in a logical manner that is not encumbered by predetermined rules. This research is based on such a premise – to understand what the key barriers are to realising the benefits of risk management.

Quantitative research may represent an area for further study that could be investigated once this research is completed. Further studies may delve into the percentage of success that can be attributed to an effective risk management programme.

1.5.2.2. Data collection

This study collected the data for the empirical component through the use of face-to-face interviews.

Population

The population for this research comprises risk practitioners in financial services entities. The respondents are restricted to those in the Gauteng region to facilitate face-to-face interviews and ease of access.

Sampling

Sampling is used in research for reasons of practicality – it would be difficult to obtain responses from the entire population due to time, cost, and logistical constraints. While the ideal would be to get as many responses as possible to validate assertions or conclusions, this needs to be balanced against what is reasonable.

The sample consists of 25 interviews with individual risk practitioners from a variety of entities, and comprises different levels of experience and organisational levels.

Interviews were conducted with risk practitioners in the Gauteng province, and therefore this study uses a combination of stratified and convenience sampling, since the Gauteng province can be considered the country's economic hub. This province is deemed to have sufficient representation of the experiences of risk practitioners on the topic of this study. The interviews were structured according to the secondary research objectives, which were as follows:

- To determine which factors impede the successful implementation of risk management. The interviews were based on the following factors:
    - personnel factors;
    - organisational culture;
    - economic factors; and
    - factors related to skills, knowledge, and training.

Demographic data was primarily used to indicate the different types of respondents consulted. It was also used to explore whether there were any differences between the responses of more experienced and less experienced respondents, or between respondents who are employed at a senior level and those at a junior level.

The research was not conducted to make reference to specific organisations, thus individuals were approached. Further, the questionnaire does not require information about their respective organisations, save for four items: "risk management within my organisation is effective"; "risk management within my organisation is a tick-box exercise"; "risk management is visible within my organisation"; and "the business strategy takes into account risk management within my organisation". Although these items are not critical to the study, they provide insightful links to the effectiveness of risk management and the factors that may influence effectiveness, such as the visibility of risk management. This may prove to be a useful area for future research. The respondents were made aware that the study was anonymous and not organisation-specific, but rather industry focused.

Interviews were primarily conducted via Skype. The interviewer plotted the responses on a rough script, and afterwards captured this in an Excel spreadsheet. The responses from the respondents were directly transcribed, and their use was strictly for the purposes of this study.

The rough scripts included the details of the respondents to keep track of the various interviews, but any indications of identity were coded as “Respondent 1, Respondent 2”, and so forth in the Excel spreadsheet to maintain the anonymity of respondents. The respondents were informed that confidentiality and anonymity would be maintained.

Data analysis

The data analysis used statistical methods in as far as they provided descriptive information regarding the responses obtained. The researcher then combined the results of the interviews and the literature review to answer the research questions.

The data analysis of the interviews was conducted in the form of a thematic analysis. Selected themes were used to form the basis of the empirical findings.

1.6. Limitations of the study

The limitations section demarcates the scope of the study, and makes known all the key assumptions that the study will be based on, and this is integral for providing the research context to the audience (Kotze, 2007). Understanding the limitations contextualises the results, so that the audience is well informed of the shortcomings of the research.

Research inherently has limitations, ranging from the use a portion of the population in the form of a sample, to the amount of literature available or consulted. The research findings will also be applicable only to a point in time, or for a period of time, as the research has a definite start and end date.

As responses were only obtained from respondents based in Gauteng, and only those who are employed in the financial services sector, the results are not generally applicable. The study furthermore aimed to obtain the perspectives of risk management practitioners, thus responses were sought from only those individuals who are required to implement, effect, or facilitate risk management.

The primary limitations of the study can be summarised as follows:

- the intention was to gain further insight into the topic and related concepts, thus no quantitative techniques were applied to the data; and

- the amount of data consulted was limited due to time constraints.

Not all available risk management standards were reviewed, since there are commonalities between the various standards. Therefore, to avoid duplicating effort, only widely adopted standards were consulted, namely the ISO 31000 and the COSO ERM framework.

1.7. Ethical considerations

Ethical considerations as guided by the NWU Research Ethics application form were duly considered in undertaking the research. The study and subject matter did not seek to obtain any sensitive data or data of an emotional nature.

In addition to respondents' anonymity being guaranteed, each respondent was advised that they had the right to withdraw from any question and/or the entire process at any time.

1.8. Chapter outline

Chapter 1: nature and scope of the study

This chapter introduces the research topic and explains why the study is undertaken. The problem statement, motivation for the research, as well as the primary research question are contained in this section. This is essentially the research proposal, and outlines the research methodology.

Chapter 2: literature review

The literature review presents the secondary data gathered from written sources, such as journal articles and other studies. The topics reviewed include root-cause analysis and risk management. Relevant existing information forms the basis of this chapter, with a view to contextualise the current landscape with regard to barriers to the successful implementation of risk management.

Chapter 3: research methodology

The techniques employed to gather data, to determine the sample, as well as the analytical approach that was followed, are presented in this chapter. The chapter

tables the actual interview content, with explanations of the content in terms of the relevance and validity.

Chapter 4: data analysis

The results of the analytical processes are presented in Chapter 4. This includes summarising the data and analysing the content, as well as formulating preliminary findings for the conclusion and recommendations.

Chapter 5: conclusion and recommendations

This chapter presents an overview of the entire study. The secondary research questions are answered, and suggestions are made in line with the secondary research objectives. This, in turn, is to achieve the primary research objective. The conclusion will summarise all the findings, and provide the researcher's recommended course of action for business to take into account.

CHAPTER 2: LITERATURE REVIEW

2.1. Introduction

The literature review is an important component of the research process, with the purpose to gain a better understanding of the research topic, based on previous studies. A considerable benefit is that the researcher need not duplicate effort. The literature review is a critical review of what has already been researched, pulling disparate strands together and identifying relationships and contradictions between previous research findings (Burns, 2008).

This chapter aims to obtain an enhanced understanding of risk management by focusing on the concepts of risk, risk management, governance, and enterprise risk management.

Management involves the tasks of planning, organising, leading, and controlling (Oosthuizen, 2007:1). These tasks are structured and undertaken so that the goals set for the organisation are achieved to the satisfaction of the stakeholders. Within the business environment, management would entail performing these tasks to realise an acceptable return on investment. Since the future is uncertain, a risk element is introduced, as the set goals have a probability of not being realised fully, thus sparking the need for risk management.

The risk management concepts explored are the generic concepts as represented by universal standards, such as International Organization for Standardization (ISO) 31000, the Enterprise Risk Management (ERM) framework of the Committee of Sponsoring Organisations of the Treadway Commission, (COSO) and the provisions of the King IV Report on Corporate Governance. While the focus of the study is on financial services entities in South Africa, it is occasionally necessary to include information outside of this scope.

2.2. Financial services in South Africa

The financial services sector in South Africa typically provides services to customers that grow, protect, or save their financial position. This includes banking, insurance, investing, retirement products, funeral products, and other similar offerings (FSB,

2017a). This is an important sector that brings surplus and deficit units (lenders and borrowers) together to create a well-functioning economy.

The financial sector is the largest contributor to the South African Gross Domestic Product (GDP), comprising 20 percent of the total nominal GDP, according to the statistics for the second quarter of 2018 (StatsSA, 2018).

The financial services sector is highly regulated, so that losses to the public are avoided as far as possible. To a large extent, this sector operates on trust. However, this cannot be blindly assumed as always inherent, thus regulation is critical to maintaining this relationship.

The sector is regulated according to a twin peaks model, with two main regulatory bodies. According to the National Treasury (2018), the first regulatory body is the South African National Reserve Bank (SARB), which enforces prudential regulation. The primary aim of prudential regulation is to protect the soundness of the financial institutions. Institutional failures do not only result in losses for the institutions, but also for clients, employees, and the economy at large; thus, the soundness of these institutions is important. The second regulatory body is the Financial Sector Conduct Authority (FSCA), which ensures conduct regulation. The FSCA has as its objective the protection of customers from unfair treatment or conduct at the hands of regulated financial institutions (FSB, 2017b).

Financial services were traditionally only offered by banks, insurers, investment houses, and other specifically established financial services entities. However, this has changed significantly. In recent times, financial services are offered by retailers, telecommunications companies, and department stores.

2.3. The financial services industry

The number of regulated, nonbanking financial services entities, as of 31 March 2017, are as follows (FSB, 2018):

- Retirement funds – 5,289
- Long-term insurers – 79
- Short-term insurers – 95
- Financial advice and intermediary service providers – 10,669

- Collective investment schemes – 1,631 portfolios
- Johannesburg Stock Exchange dealers – 3,902

The number of banking institutions, as regulated by the SARB, are as follows (SARB, 2018):

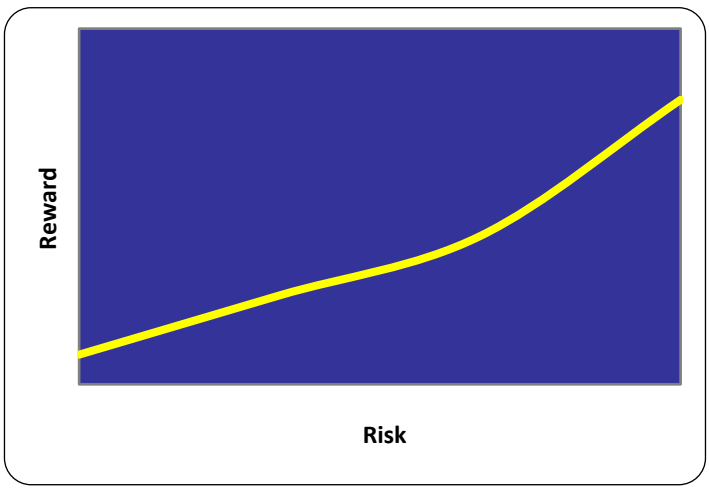
- Locally controlled banks – 11
- Mutual banks – 3
- Foreign-controlled banks – 7
- Foreign bank representatives – 29
- Branches of foreign banks – 15
- Banks in liquidation – 2

2.4. Risk and risk management

The International Organization for Standardization (ISO) ISO 31000 report (2018:1) defines risk as the effect of uncertainty on the outcome of objectives. The focus is ultimately the objectives of the organisation – all performance (good or bad) is measured against the objectives set. Risk management, by deduction from the risk definition, entails all planning, organising, leading, and controlling activities aimed at ensuring that objectives are met, taking into account the uncertainty that the business faces.

The notion is that as risk increases, so too does the potential reward (Dhankar, 2006:23).This is represented in the Figure 2.1, which shows the relationship between risk and reward.

Figure 2.1: the risk-reward relationship (adapted from Dhankar, 2006)



It is important to note that the correlation between the two variables is not necessarily always a coefficient value of 1 (that is, a 45 percent increase in risk does not necessarily equate to a 45 percent increase in the potential reward).

Historical interactions with line management have highlighted a common misconception that risk management means elimination of all risk. In fact, risk management entails making those decisions and implementing those risk response strategies that will ensure that the risk the entity is exposed to, falls within the risk appetite of the entity. This involves conducting numerous risk-reward analyses.

2.5. Components of risk management

The FSCA, in its Financial Advisory and Intermediary Service (FAIS) risk management newsletter (2010:4), defines risk management as the process involving identification, assessment, prioritisation of risks, and applying resources to minimise, monitor, and control the extent and/or likelihood that negative or undesirable results manifest.

There are a number of risk management models which exist, each with basically the same key components: risk identification, risk monitoring, risk responses, risk evaluation, and risk reporting. The COSO risk management model is one of the initial models established, and is still widely applied and relevant in today's environment. The COSO was formed in 1985 as part of the Treadway Commission's efforts to review the causes of fraudulent financial reporting (COSO, 2011).

The COSO model consists of eight components that effectively encapsulate all risk management activities, discussed below. (COSO, 2004:3-4).

2.5.1. Internal environment

The culture within the organisation should be of such a nature that risk is understood by all, and this understanding must be consistent across the entity. There needs to be awareness in business as to what risk means in the context of day-to-day management activities (COSO, 2004:3-4).

2.5.2. Objective setting

When determining objectives and subsequent strategies to realise those objectives, the risk appetite must be taken into account. Simply put, risk appetite is the amount

and type of risk that an organisation is willing to absorb in pursuing its objectives (SABS, 2009:9). The risk appetite establishes the acceptable range of risks and amount of risk within which the entity can operate. An example of this is a bank that sets a risk appetite of a fraud-loss ratio up to 0.5 percent of revenue. The risk appetite in this example is illustrated by scenarios 1 and 2.

SCENARIO 1: Total fraud losses equal R1000 and total revenue equals R250,000. The fraud loss ratio is 0.4 percent. This is an acceptable fraud loss ratio, as it falls within the appetite set.

SCENARIO 2: Total fraud losses equal R2000 and total revenue equals R250,000. The fraud loss ratio is 0.8 percent. This is an unacceptable fraud loss ratio, as it exceeds the appetite.

The risks inherent in the decisions taken must be compared against the risk appetite, and the ultimate decision should be driven by the risk-reward consideration (Chapman, 2006:9).

2.5.3. Event identification

There should be a common understanding of what constitutes a risk event. A risk event represents the manifestation of a risk. Essentially, this would be an event that has an impact on set objectives. An example of this, is as follows:

- Risk: the risk of internal fraud being committed; and
- Risk event: an internal fraud of R50,000 is discovered by auditors.

According to the Chartered Institute of Management Accountants (CIMA, 2006) more often than not, the focus is on those events that could have a negative impact on the objectives. This is not to say that upside risks do not exist in the form of opportunities – these too, must be identified and leveraged for goal maximisation. Risk management relies on learning from historical events and making use of data to inform of potential future risk exposures, and this can be facilitated by maintaining a loss event database. Such a database would record the details (per predefined categories) of loss events in a manner that allows for aggregation, as well as detailed dissection. Consistency is critical here, especially if a database of incidents is maintained and used for analytical purposes. Consistency will ensure data integrity and completeness.

2.5.4. Risk assessment

The risk is quantified, taking likelihood and impact into account. Likelihood is the probability or chance that the risk will occur, and can be influenced by frequency. Impact refers to the consequence or result that would be realised if the risk were to materialise. The product of likelihood and impact will yield a risk rating. A risk rating be done at an inherent level as well as at a residual level. Inherent risk rating refers to the risk rating without taking into account dedicated controls, whereas the residual risk rating takes cognisance of all controls and their effectiveness to arrive at a residual risk rating (FirstRand Banking Group (b), 2011).

2.5.5. Risk response

There are four risk treatments available to management, characterised by the 4 Ts: **t**ake the risk, which entails accepting the potential risks and rewards; **t**erminate the risk by withdrawing from the activity or business that gives rise to the risk; **t**reat the risk by implementing control measures to reduce the risk to within acceptable levels; or **t**ransfer the risk via joint ventures or insurance. The risk response selected is dependent on the risk appetite (CIMA, 2006).

2.5.6. Control activities

A system of internal controls is established in such a way that the risk exposures do not exceed the risk appetite set by the board. These controls can be in the form of policies, processes, or physical controls. In the implementation or deployment of controls, a cost-benefit analysis must be undertaken to ensure that the benefit from implementing same exceeds the costs of doing so (CIMA, 2006).

2.5.7. Information and communication

Relevant information and the timely communication thereof is important at all stages of the risk management process, because information is required to make informed decisions at each stage. The communication mechanisms must ensure that the message is clear, easily understood, and not ambiguous (CIMA, 2006).

2.5.8. Monitoring

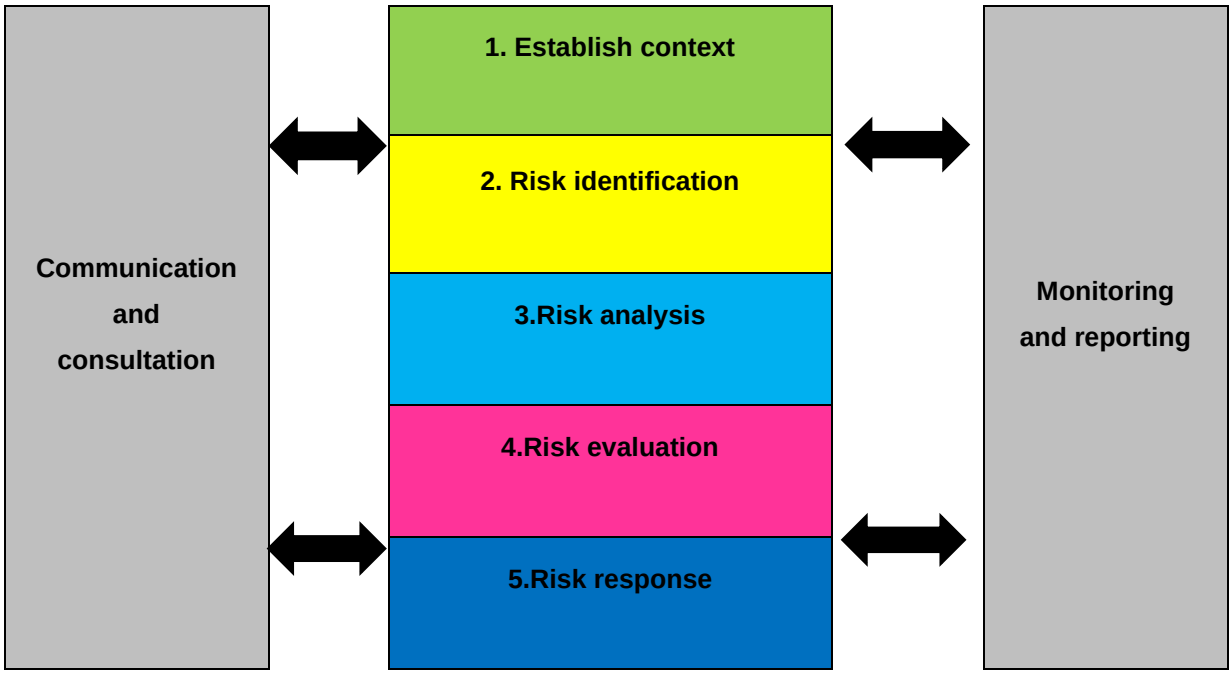
Continuous monitoring of the effectiveness of the embedded risk programme, and the risk and control environment, must take place. Where results are unsatisfactory, the risk response decision will be required to amend the risk exposures (CIMA, 2006).

2.6. Generic risk management model

While organisations may have different naming conventions for each of their risk management activities, they will to some extent mirror the stages of the COSO model. The model is still highly regarded as an effective approach to implementing an ERM model, thus an assessment as to whether an entity's risk management function is effective or not, can be performed by using the model as a benchmark.

Organisations typically have a standard risk management model comprising similar activities. Below is a generic risk management model that represents a summarised version of the COSO model.

Figure 2.2: Generic risk management model (source: IRM, 2010).



The ISO 31000 risk management model (IRMSA, 2014) puts forth the following components and explanations for the risk management process:

2.6.1. Communication and consultation

This step is concerned with ensuring that the right information reaches the right recipients at the right time. The applicable stakeholders and their information needs must be identified upfront, so that these expectations are met as the process unfolds. The provision of timely, accurate information is necessary to avoid perceptions based on rumours, misconceptions, or half-truths (IRMSA, 2014:34). An example that illustrates this stage, is the establishment of a monthly forum that consists of representatives of all three lines of defence (discussed in section 2.7). This forum would discuss the risks (according to the risk register) and progress in terms of resolving risk items. The forum would serve as a form of consultation, with participants such as the risk management function providing advice on control adequacy and effectiveness.

2.6.2. Establish context

Risk should be contextualised so that it is relevant to what the organisation deems important. Establishing the context speaks to understanding the organisational

objectives, and using them as the departure point for risk management, since the definition of risk is premised on objectives. The context considerations should cover both internal and external environments. The external context focuses on the external forces on the organisation, typically identified as macroeconomic as well as social, political, technological, environmental, and legislative factors (IRMSA, 2014:33). For example, the context can be set by having the risk management function involved in the strategy process. This would provide information on the strategic direction of the entity as well as where resources should be allocated. Such information on the objectives of the entity assists the risk identification process, ensuring the alignment of risk identification to what is strategically important to the entity.

2.6.3. Risk identification

The first step in the risk assessment stage is the identification of risks. The primary aim is to have a complete, relevant, and accurate record of the risks that are inherent in the organisation. This step is highly dependent on information from the previous step, as well as the input from the risk owners (typically line management). The identification of risks can be informed by a myriad of sources, such as a loss database, external databases, regulatory processes, management self-assessments, audit findings, or SWOT analyses, to name a few (IRMSA, 2014:36). An important requirement to ensure that risk identification is undertaken successfully, is a common risk language, so that all participants have a common understanding of what risk is (IRM, 2018:15).

Risk identification and root-cause analysis

The importance of risk identification cannot be overstated, since it is the starting point of many other steps in the risk management process. Starting off incorrectly is likely to yield inadequate results. This is encapsulated succinctly by John Dewey (as cited by Christodoulou, 2005:18) in his quote “[a] problem well put is half-solved”. Therefore, when identifying risks and potential mitigating measures, it is imperative that the root cause of the risk is understood. The section that follows explains what a root-cause analysis is, and why it is necessary.

A root-cause analysis is a process that makes use of data and/or information from a variety of sources to identify the basic reason(s) for the appearance of a problem, and in attempting to identify the root cause of a problem, certain hypotheses are formed; subsequently, data is collected to confirm or refute these hypotheses (Horev, 2009). One thing that needs to be understood, is that not all problems can always be reduced to a single root cause. Regardless of the sophistication of the models being used, cognisance must always be taken of multi-causal phenomena, which makes identifying a single root cause extremely difficult (Garavaglia, 2008).

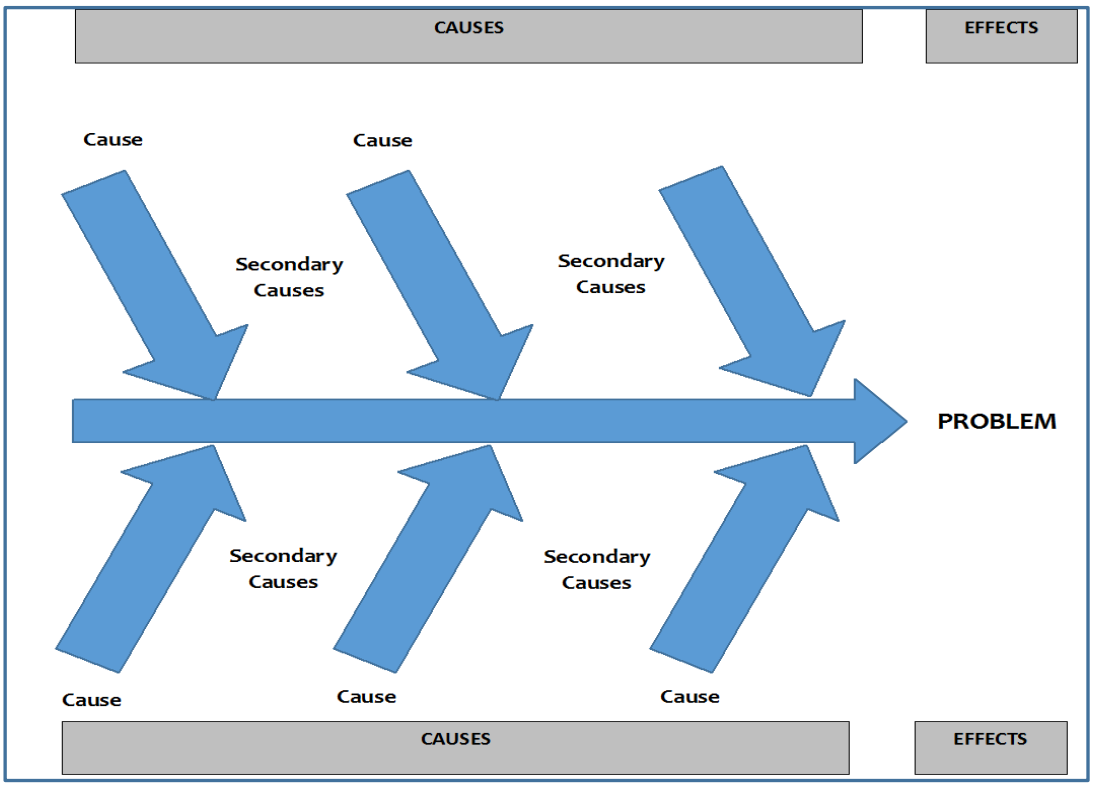
In a study concerning the human aspect of root-cause analysis, Okes (2008) postulates that although technology and models are available to facilitate the process, a root-cause analysis is ultimately a cognitive process influenced by human emotions, historical experiences, and biases. This requires that the sponsor of the root-cause analysis has detailed knowledge of the team: their backgrounds, areas of strength (which they will inadvertently tend to lean towards), and their cognitive skills, in such a way that the potential biases can be identified upfront, and measures put in place to avoid biases, or that biases are taken into account when interpreting the generated results. This is a crucial point to understand when conducting a root-cause analysis.

An entity should seek to identify the causal factor that it can influence, and seek to address this. For example, if funds are lost after a bank branch is attacked by armed robbers (with no employee involvement), the source of the attack is external (the robbers), and the impact is financial loss (funds/money). The usual root cause is identified as external criminal activity. When we consider the causes for external criminal activity, they are likely poverty, improper morals, lack of education, and so on. None of these factors is within the direct control of the bank branch, thus the root cause does not yield valuable output. In this instance, the bank should take into account the controls and processes in place to protect it against armed robberies – the focus then shifts from simply marking the incident cause as external to internal controls. The root-cause analysis may then identify causes such as lax physical security controls, which is in turn caused by poor training of security guards. This represents a variable that the bank has potential influence over, and addressing this is more likely to mitigate the risk of future robbery losses.

The root-cause analysis is inherent in the problem-solving process. Organisational problems are risks that could hamper success. Where actual performance is not in line with planned performance, it is safe to assume that some sort of problem exists. A study investigating the informational needs of students for solving a set of problems, revealed that problems that were identified and defined well, required less effort, as opposed to a situation where the problem was not defined adequately (Laxman, 2010). This affects the efficiency of operations within an organisation, and potentially the effectiveness of the mitigation actions that are implemented.

The Ishikawa diagram (shown in Figure 2.3), developed by Kaoru Ishikawa, is a common tool used in conducting root-cause analyses. The tool makes use of a fish skeleton diagram to analyse a particular problem – the problem experienced is the effect (head of the fish) and the potential underlying causes are represented by the bones (Wong, 2011).

Figure 2.3: Example of the Ishikawa diagram (source: RFF Electronics, 2010).



Although the Ishikawa diagram and other similar models are easy to use and offer solutions if applied correctly, difficulties arise where multiple root causes are identified as the underlying risk. This may necessitate further brainstorming analysis to

investigate any relationships between the root causes identified – one root cause may in fact be the effect of another root cause identified.

The organisation must take note of the weaknesses of models used to identify root causes, to avoid unwanted results generated by the process. The proactive risk managing organisation is the one that will undertake root-cause analysis exercises up to the point where it has relative influence over the underlying risk identified.

For root-cause analysis to yield valuable results, it must include the participation of senior management and those familiar with the associated processes and systems, and there should be consistency in approach throughout the organisation (Uberoi, 2004). The various root-cause analyses results will serve as input to establish criteria for the root-cause-analysis process within the entity

2.6.4. Risk analysis

Risk analysis involves gaining an in-depth understanding of the risk exposure. Understanding risk exposure is necessary to make decisions regarding risk treatment and the prioritisation of resources. Risk analysis entails using information to determine the level of risk that exists. When determining the varying levels of risk, it is possible to make informed decisions in terms of prioritisation of resources, as well as urgency-related decisions. In order to achieve this, the likelihood of the risk manifesting, as well as the associated impact of the risk, should it materialise, must be determined (IRMSA, 2014:39). The risk-analysis step becomes more meaningful if the impact of the risk can be related to the organisational objectives identified during the step that entails establishing context – this assists in identifying the key risk exposures. The determination of key risk exposures will be based on the risk prioritisation – those risks that pose a bigger threat to the realisation of objectives will be prioritised over risks with a lower potential threat. To ensure that consistent risk analysis is undertaken throughout the organisation, the use of risk rating scales or matrices is recommended. These matrices define consistent measurement parameters for each rating (IRMSA, 2014). Figure 2.4 provides an example of a risk rating matrix for risk impact and risk likelihood. Figures 2.5 and 2.6 are supporting figures that provide examples of definitions for each of the risk ratings.

Figure 2.4: Example of a likelihood rating scale (source: Bayport Management, 2018:5).

Likelihood/probability		
5	Almost certain (80-100%)	Expected to occur in most circumstance (almost regularly).
4	Highly likely (60-80%)	Will probably occur.
3	Likely (40-60%)	Could occur at some time.
2	Unlikely (20-40%)	Could occur in isolated instances.
1	Rare (1-20%)	Will only occur in exceptional circumstances.

Figure 2.5: Example of an impact rating scale (source: Bayport Management, 2018:5).

Impact		
5	Catastrophic	An impact which is considered to be beyond the stakeholders' ability to manage or resource, and as a result, threatens the survival of the entity.
4	Significant	The impact would threaten the ability to achieve objectives in the medium term.
3	Moderate	The impact would threaten the ability to achieve objectives in the short term.

2	Minor	The impact would pose a minor threat to the ability to achieve objectives.
1	Insignificant	The impact could be absorbed within the day-to-day business-running costs.

Figure 2.6: Example of a risk rating matrix (source: Bayport Management, 2018:5).

Impact	**Likelihood**				
	Rare (1)	**Unlikely (2)**	**Possible (3)**	**Likely (4)**	**Almost certain (5)**
Catastrophic (5)	High (5)	High (10)	Unacceptable (15)	Unacceptable (20)	Critical (25)
Significant (4)	Tolerable (4)	Tolerable (8)	High (12)	Unacceptable (16)	Unacceptable (20)
Moderate (3)	Acceptable (3)	Tolerable (6)	Tolerable (9)	High (12)	High (15)
Minor (2)	Acceptable (2)	Acceptable (4)	Tolerable (6)	Tolerable (8)	Tolerable (10)
Insignificant (1)	Acceptable (1)	Acceptable (2)	Acceptable (3)	Acceptable (4)	Acceptable (5)

The risk rating is determined as the product of impact and likelihood (mapped on the matrix in Figure 2.6). For example, a risk with an impact of Moderate (3) and a likelihood of Likely (4) will yield a risk rating of High (3 x 4 = 12).

The assessment of impact and likelihood (the product being the risk rating) must take into account the controls applied. Chartered Accountants Australia and New Zealand (CAANZ, 2016:1) define controls as any actions taken by management which either

reduces the likelihood of a risk event occurring, or reduces the potential for damage arising from that risk event. Controls can include any process, policy, device, practice, or other action that modifies the risk. Line management plays a vital role in providing the information regarding the risk control measures in place, as well as assessing the effectiveness thereof. Control measures are specific interventions, actions, or processes implemented to address risk exposures. Assurance providers (second and third lines of defence, section 2.7.) should challenge the assessments of control effectiveness, based on information that they have at their disposal. The example in Figure 2.7 explains controls and control effectiveness.

Figure 2.7: Example of control and control effectiveness

RISK	The risk of burglars gaining access into an office and stealing laptops.
CONTROL	Security guards that control access to the office building.
EFFECTIVE CONTROL	The guards perform their duties according to the standard operating procedures, and no theft occurs.
INEFFECTIVE CONTROL	The guards sleep while on duty, and ten laptops are stolen.

2.6.5. Risk evaluation

Evaluation of the risk is required to prioritise risks, and this has to be undertaken with consideration given to the organisational objectives. The evaluation of risks is usually against predetermined criteria for decision making (IRMSA, 2014). The prioritisation is guided by the risk rating per the risk rating matrix (Figure 2.6). A risk with a rating of Critical (25) will be prioritised over a risk with a rating of Tolerable (9), since the potential to threaten the achievement of objectives is higher in the case of the critical risk. The prioritisation is also guided by the risk appetite set by the board. Risks that are close to the appetite limits, or exceed the appetite, will be prioritised over of those that are well within appetite.

2.6.6. Risk response

Once the risks have been identified and assessed accordingly, decisions for further actions (if any) are required to bring the risk exposures within acceptable levels – these are the risk responses. The acceptable level of risk is determined by the risk appetite that has been set. According to the Association of Insurance and Risk Managers (The Association of Insurance and Risk Managers, 2010: 16) risk appetite is a concept that explicitly states the types of risks, as well as the amount/level/quantum of risk, that is acceptable to the entity. According to CAANZ (2016) there are a number of risk response decisions that can be implemented. (CAANZ, 2016). Using the earlier example of a fraud-loss ratio appetite of 0.5 percent of revenue (section 2.6.2.) and the risk response decisions set out by CAANZ (2016), the first option is to **avoid** the risk. An entity may choose not to be involved in the activity that gives rise to the risk, or opt for a different alternative. This is also referred to as termination of the risk. For example, if it is determined that the fraud-loss ratio from a specific market is 3 percent of revenue, the decision to terminate operations within that market may be justified, since the appetite (0.5%) is exceeded by 500 percent. The risk response decision would be to avoid the risk. The second option is to **reduce** the risk. This entails introducing or implementing measures to reduce the likelihood or impact of the risk to a level that is acceptable to the organisation, essentially to within the risk appetite. For example, if the fraud loss ratio is 0.7 percent, the decision to introduce more controls may be taken in order to reduce the ratio so that it falls within the risk appetite of 0.5 percent. This may be in the form of additional fraud checks, additional staff employed, or a reduction in sales. Third, an entity can choose to **transfer** or **share** the risk. To achieve this, strategies that allow for the risk to be shared are implemented. Risk transfer is effected through outsourcing, insurance, or contractual provisions. The entity may choose to share the risk (limit the risk exposure to a certain level) by insuring losses above a certain level. For example, the entity may choose to insure losses above R50,000, thus limiting their loss value to R50,000 per incident. Finally, the entity may **accept** the risk. They may decide that the level of risk is within the risk appetite of the organisation and accept it. No further mitigating actions are deemed necessary, as the benefits are deemed to exceed the disadvantages. This would be the case if the fraud loss ratio is 0.4 percent. This is within the 0.5 percent risk appetite

limit that has been set, and no additional control measures are implemented. The decision is taken to accept the risk as is.

2.6.7. Monitoring and reporting

The old adage, “what gets measured, gets done,” holds true for risk management as well. There has to be a continuous review of what the aggregate risk exposure is, and how the entity fairs with keeping risks within its risk appetite. New circumstances that may affect the risk evaluation or risk assessment should be identified, communicated, and recorded in order to make informed risk response decisions (CAANZ, s.a.:1)
The risk management processes, as outlined by the different standards, provide similar guidance, following a pragmatic, step-by-step process for gathering and analysing sufficient information in order to make informed decisions as far as risks are concerned.

2.7. Risk Management within South Africa

Risk management within South Africa is on a path of continuous improvement. One merely has to sift through job search sites or vacancies placed in newspapers to notice the demand for risk management skills in the public and private sectors alike.

Since risk management is dependent on the inherent risks identified, a good departure point is the Top 10 South African risks as identified by IRMSA (2019:6). IRMSA is arguably the leading body advocating and driving risk management advancement within South Africa, with a wide membership base and being recognised by The South African Qualifications Authority as the professional body for the discipline within the country (IRMSA, 2019:1). The list below outlines the Top 10 risks and also the salient impacts that these risks could potentially have, more specifically on private sector entities:

1. Structurally high unemployment: higher unemployment has a number of direct and indirect impacts on businesses, from potentially increased levels of crime to reduced business income due to less buying power from the unemployed population.
2. Growing income disparity and inequality: income disparity would have to be addressed at some point either by reducing income that is too high (which

may lead to labour disputes or resignations) or upwardly adjusting income that is too low (this could have a significant impact on profitability and sustainability. These disparities may also introduce lower morale or staff protests.

3. Failure of governance – public: lack of accountability and governance within the public sector space eventually spills over to the private sector, since the incentive to implement good corporate governance becomes non-evident.
4. Unmanageable fraud and corruption: fraud and corruption if not addressed runs rampant especially where other problems such as unemployment and inequality exist – these problems being used as justifications to these criminal acts. Fraud affects profitability and reduced profit affects the ability of businesses to reward their employees and shareholders as well as reducing the ability to contribute towards reducing unemployment.
5. Inadequate and/or sub-standard education and skills development: the lack of adequate skills impacts the ability of businesses to develop competitive advantage, innovative solutions and robust businesses. There are additional costs of having to upskill employees or ultimately having to introduce performance management interventions which may fail leading to recruitment once again (costs, time and lost productivity).
6. Energy price shock: electricity is an input factor in the delivery of products and services. Electricity price increases at any point in the value chain result in further costs being experienced throughout the rest of the value chain and ultimately by customers. Higher prices could result in consumers exploring alternative suppliers (foreign suppliers due to increased globalisation) or substitute products.
7. Labour unrest and strike action: workforce instability affects productivity and the customer experience. The nature of labour unrest in South Africa is that it is coupled with intimidation and violence from time to time. Lost working days for 2017 was quoted by the Department of Labour as being 960,889 days which was an increase of 1.5 percent from the 2016 year (Department of Labour, 2018:8). These lost days result in lost business and backlogs.
8. National political uncertainty/instability: political instability has the potential to scare off or delay investment in the country, reducing the flow of funds and the number of potential opportunities that businesses could take advantage of.

Increased levels of uncertainty similarly delay decision making in instances where the increased risk levels are deemed unacceptable.

9. Cyber-attacks (ransom, algorithm shutdown of the internet of things): as technology develops and more items are connected to the internet, the more cyber-attacks are likely to occur. Since South Africa may be lagging behind other countries in technology advancement, security and importantly user awareness and education it is likely that this risk will become more prevalent going forward. The South African Banking Risk Information Centre (SABRIC) estimates that R2.2bn is lost annually in South Africa due to cyber-crime (SABC News, 2018). SABRIC also note a 44 percent increase in online banking incidents when January to August 2018 is compared to the same period in 2017 (SABRIC, 2018). This is largely attributed to phishing scams.
10. Macro-economic developments: macro-economic changes such as currency depreciation, higher inflation and a high interest rate regime would impact the profitability. In certain instances the impact would be direct (e.g. foreign exchange losses) as opposed to indirect (e.g. higher operating expenditure due to inflationary price increases of goods and services). Lower GDP growth would also mean potentially less purchasing power from consumers, depending on the elasticity of the relevant products/services. Entities operate within the wider economy and are thus not immune to macro-economic issues.

The key drivers of risk management within South Africa are as follows, from a regulatory or standards perspective:

1. King Code on Corporate Governance: the King Code on Corporate Governance is regarded as the standard and benchmark with regards to Corporate Governance within South Africa. The Code is highly regarded and is a Johannesburg Stock Exchange requirement for listed entities – on an “apply and explain” basis in terms of the Code requirements/principles (Institute of Directors Southern Africa, 2018)
2. Public Finance Management Act (PFMA): Accounting officers within public sector entities or departments are responsible for risk management as per Section 38 of the PFMA, Act No. 1 of 1999 (National Treasury, 1999).

Further detailed guidance is provided by the Public Sector Risk Management Framework maintained by the Office of the Accountant General (National Treasury, 2009). This not only impacts how public sector entities operate, but also the interactions with private sector entities.

3. The Twin Peaks Model: the Twin Peaks model is represented by two important “pillars” of the South African financial system (National Treasury, 2018):
    a. Prudential authority – this entity, which is housed within the South African Reserve Bank will be responsible for supervising the safety and soundness of all financial institutions.
    b. Financial Sector Conduct Authority (Previously the Financial Services Board) - this entity will be more focused towards consumer protection, and will supervise financial institution conduct.

The twin peaks model aims to embed a comprehensive financial sector supervision and governance regime within South Africa by building upon and strengthening many existing entities. The South African financial sector was deemed to be well governed and supervised following the 2008 Global market meltdown, having not been subject to as extensive negative impacts as other, more-developed jurisdictions.

2.8. The impact of Technology Risk

Technology, as an enabler, is fast becoming intertwined in each aspect of business and private life. Technology has resulted in many advances in business, healthcare, everyday living, education etc. Whilst technology has introduced numerous benefits such as convenience and ease of access this does not come without risks. Developments such as internet banking have made it easier, faster and more convenient for South African consumers to perform banking activities that in the past required them to physically be in a bank branch (often in long queues). Additionally, bank branch hours are restricted to certain times whereas internet banking can be conducted at any time of the day – adding to the convenience and benefits “business-case” of technological advancement.

Internet banking does however introduce new threats and methods of criminality. Technologically advanced criminals utilise cyber-crime capabilities to perpetrate what is essentially “faceless” criminality. This makes it an attractive proposition to criminals

since they can commit crimes remotely, without being identified or having to plan elaborate escapes from authorities.

Cyber-threats have been identified as a Top 10 Risk for South Africa as a country, by The Institute of Risk Management South Africa, for 2018 and 2019 (IRMSA, 2019:7).

The 2018 Banana Skins Financial Inclusion report has identified Technology Risk as the Number One (1) risk (Centre for the Study of Financial Innovation, 2018:1). The report is derived from 300 responses across 70 countries, including amongst others regulators, investors and other practitioners. Noteworthy is the fact that Technology risk was identified as the Top risk specifically in the Africa and Latin America regions – this would include South Africa, and become more applicable to South African entities embarking on African expansions.

The 2017 Banana Skins Insurance report (Centre for the Study of Financial Innovation , 2017:7) has identified Cyber Risk as Number Two (2) and Technology Risk as Number Three (3) in its survey.

The pervasive nature of technology would assumedly give rise to more risk, and this is corroborated by the various risk and business surveys undertaken periodically. This not only influences the demand for Enterprise Risk Management, but also for the niche IT risk management.

2.9. The 4th Industrial Revolution

The 4th Industrial Revolution is a term that is being widely discussed and receiving ever-increasing focus. World Economic Forum Co-Founder and Chairman, Professor Klaus Schwab notes that whilst technological advances have taken place in previous industrial revolutions, the 4th revolution is characterised by fundamentally different and significant change (World Economic Forum, 2019). The new technologies now being developed have a wider reach fusing the physical, digital and biological spheres.

The potential benefits of being able to more easily connect more humans and devices and also the potential for significantly improved efficiency does not come without associated risks. Inability to adapt to new technological advances and failure to adequately regulate these are noted as some of the more salient concerns (World Economic Forum, 2019).

Within the South African context the 4th industrial revolution has resulted in fast-paced technological innovation within the financial services sector to the extent that Fintech growth presents real competitive threats to traditional financial services entities.

The technological advances that the revolution is able to introduce can yield significant efficiency, but the following risks have been identified as being especially relevant within the South African financial services sector (Centre of Excellence in Financial Services, 2017:2):

- Regulatory risk – regulation to protect the financial system's soundness as well as consumers is required and this has to match the pace of the change. The research conducted by the Centre of Excellence in Financial Services (COEFS) indicates a historical tendency for regulators to focus their efforts predominantly on consumer protection – this might be at the expense of innovation progression.
- Operational risks (cyber-security and technology failures) – with increased connectedness and options for transacting, there is a resultant increased potential for cyber-attacks to be perpetrated. Research undertaken by renowned cyber security firm Kaspersky Lab in 2019 shows that South African Android devices are the second most targeted in the world, behind only Russia (Smith, 2019). The number of daily attempted cyber attacks equates to approximately 13,800 per day or put otherwise, approximately 9 attacks per second. The impact of technology failures becomes dramatic due to the extensive reliance on technology – this is further exacerbated by the dependence on electricity, the supply of which is erratic at times within South Africa.
- Exclusion of certain societal segments – whilst technological advances associated with the industrial revolution make certain functionality more accessible, the socio-economic factors within South Africa still make it difficult for many segments of the population to benefit therefrom. The following South Africa specific socio-economic factors result in only a portion of the population being able to benefit from innovation realised as part of the revolution:
    - Limited access to internet connectivity in rural areas,
    - lack of access to smart phones or computers,

- illiteracy and a limited number of individuals that are financially savvy, and
- income inequality.

The risk herein is that entities invest large amounts of capital in new technology that is not widely taken up or not adequate for the target market.

- Skills requirements – dramatic change in technology introduces a demand on new skillsets to be able to develop, use and support such technology. There is also the potential of job redundancies where certain jobs are either no longer required or can be done much better by technology. In a country where skills shortages have been experienced in key sectors, this introduces the risk that recruiting for the required skills will be difficult and potentially costly due to low levels of supply for a high demand. These skills may also be prone to moving around more often to capitalise on better salary offers which introduces continuity risks to the entities concerned.
- Losses in the value chain - whilst the South African financial services sector is regarded as developed, certain services or even skillsets may have to be sourced internationally and this results in lost value in the South African value chain.

The COEFS report authors conclude that whilst the South African Fintech sector is regarded as sophisticated and ranks highly on the African continent, there is still the possibility of significant improvement if regulators create an environment that enables and encourages the adoption of newer technologies. Since this is usually pioneered by entrepreneurs and start-ups, more focus should be placed on assisting them to overcome hurdles such as bureaucracy and over-bearing regulatory requirements (COEFS, 2017).

2.10. The three-lines-of-defence model

As with any other business activity or function, the allocation of responsibility and accountability is important in driving the implementation of requirements. Accountancy South Africa (ASA, 2014:1) sees the responsibility of the board of directors as that of a risk governance body. The risk governance responsibilities of the board of directors

includes setting the risk appetite, monitoring strategic alignment, and defining the overall risk management expectations.

Organisations, especially larger organisations that comprise thousands of employees and multiple locations, have a number of stakeholders, each responsible for contributing towards the achievement of objectives. In this very same way, each stakeholder contributes to risk management. The responsibilities for risk management are typically depicted in the three-lines-of-defence model. An outline of the model, as set out by the Institute of Internal Auditors (IIA, 2013:3-6) is subsequently discussed.

2.10.1. The first line of defence: operational management

Operational management manages and owns risks within their areas of responsibility, and are thus responsible for maintaining an effective internal control environment. Since controls are embedded into day-to-day procedures and systems, it is fitting that operational management is regarded as the first line of defence, “at the coalface” (IIA, 2013:3).

2.10.2. The second line of defence: risk management and compliance functions

The second line of defence serves to ensure that the activities of the first line of defence are monitored, to assist in maintaining an effective internal control environment. This is commonly undertaken through monitoring activities. The second line of defence is typically characterised by the establishment of three functions, each with a specific area of responsibility (IIA, 2013:4). The first function is a **risk management function** that facilitates and monitors the implementation of the risk management process within the business through close interaction with the risk owners. It is important to note that the risk management function does not assume the role of the risk owner, rather, it assists in embedding a robust risk management environment. The second function is a **compliance function** that also facilitates and monitors the implementation of a robust risk management process, but more specifically for risks of a regulatory or legislative nature. Regulatory risk, and the risk of regulatory change, has frequently featured in IRMSA risk surveys (IRMSA, 2018). It is therefore important that a specific focus is allocated to such risks. An additional motivation for having a separate compliance team that undertakes compliance risk

management, is that many entities (especially financial services entities) are dependent on licenses to operate, and such licenses require compliance with regulation. The final function is a **controller function** for risks of a financial nature. The controller function is predominantly focused on ensuring accuracy, validity and integrity of the financial functions as well as the output thereof – the financial reporting.

According to the IIA (2013:4) the second line of defence is intended to be independent of operations so that objectivity is maintained and provides valuable assistance to operational management through the following actions:

- establishment of risk management frameworks (this can be at the level of specific risks, such as regulatory risk management frameworks);
- providing input for controls to be considered in processes;
- providing management with input regarding emerging risks and risk themes;
- the development of tools and templates to be used to implement the risk management process;
- monitoring the adequacy and effectiveness of control; and
- advising regulatory change and performing gap analyses.

2.10.3. The third line of defence: internal audit

Independent assurance with regard to the internal control environment is provided by the internal audit function. This assurance serves as valuable input to the board of directors and senior management, since there is a greater element of objectivity attached to the assessments performed by an internal audit. The IIA (2013:5) notes the following requirements for best practice:

- adopting and adhering to recognised international internal auditing standards;
- the reporting line of the internal audit function should be to a senior level within the entity; and
- an internal audit should have a reporting line to the governing body.

Ensuring that all these lines of defence interact in a manner that contributes to an efficient and effective risk management and assurance environment, is ultimately the premise behind the concept of combined assurance. King IV (Institute of Directors Southern Africa, 2016:10) describes the combined assurance model as a model that

incorporates and optimises all assurance services and functions so that, taken as a whole, these enable an effective control environment, support the integrity of information used for internal decision-making by management, the governing body, and its committees, and support the integrity of the organisation's external reports.

King IV (Institute of Directors Southern Africa, 2016:68) proposes a lines-of-assurance model that does not differ materially from the three-lines-of-defence model, but it includes additional assurance providers as part of the model. The King IV model includes the following six lines of assurance:

1. operational line management;
2. risk and compliance functions'
3. internal audit, internal forensics functions, safety functions, and statutory actuaries;
4. independent external assurance functions (e.g., external auditors);
5. other external assurance providers (e.g., external actuarial functions); and
6. regulatory inspectors.

2.11. Risk management requirements according to regulators

Financial services regulators have formalised the requirement for regulated entities to undertake risk management in line with their primary objectives of protecting the broader financial system, as well as customers. The FSB (now the FSCA) outlines the requirements for regulated entities (financial services providers) to implement risk management in the FSCA FAIS Notice 54 of 2018 (FSCA, 2018).

Board Notice 158 of 2014 (applicable to short- and long-term insurers) prescribes the risk management requirements for insurers. The document outlines the structures, policies, procedures, and human resource requirements for risk management to be effectively implemented by insurers (FSB, 2014).

As prudential regulator, the SARB also prescribes risk management requirements for banks. The SARB is a member of the Basel Committee on banking supervision of the Bank of International Settlements. The primary mandate of the committee is to ensure financial stability through robust supervision and regulatory practices, with one of the key functions being identifying weaknesses that pose risks to financial stability (Bank for International Settlements, 2018).

Bank risk management requirements are largely driven by Basel standards, since these determine the amount of capital that banks are required to hold. The Basel standards incentivise good risk management by requiring banks to hold less capital if their risk management programmes are deemed more mature.

The Basel Committee on banking supervision has developed three different capital measurement approaches (each with its own requirements and benefits) that banks are allowed to use in determining their capital requirements – these are documented in the Basel Capital Accord (Bank for International Settlements, 2001). Banks are required to hold sufficient capital that will be able to cover expected and unexpected risks, which manifest in the form of losses.

Risk management within the South African banking industry contains many similar practices, in that it is governed by the SARB. The SARB imposes a variety of standards that banks must adhere to, so that the funds that banks safe-keep on behalf of the public are not placed under undue risk. The SARB has a supervision department whose primary objective is the protection of public deposits held at banks (SARB, 2012). The SARB further has a number of supervisory techniques, one of which is on-site visits conducted at the respective physical bank locations, during which the central bank engages with senior leadership in an attempt to satisfy themselves of that bank's sustainability.

The SARB also imposes binding legislation on all banks in the form of the Bank's Act (Act no. 94 of 1990). The Bank's Act sets out the parameters within which a bank should operate, and also determines the minimum corporate governance standards to be applied, which include the risk management function (SARB, 2007). The Act further prescribes the relevant risk management requirements for all entities granted a banking license. These include the establishment of a risk management function, the establishment and maintenance of a risk and capital management committee, and the implementation of suitable risk mitigation strategies, so that the risks assumed are within tolerable levels (SARB, 2007).

2.12. The cost of risk management failure

A key concept of risk management is learning from the mistakes of others, and using these lessons to avoid similar errors. Thus, it is important that risk management

failures experienced by other entities, or in other territories, are used as case studies to enhance risk management. Risk management failures typically manifest in the form of financial losses or (in extreme cases) the collapse of the entity.

Large corporate scandals and failures abroad have highlighted risk management weaknesses that other entities should take cognisance of if they are to minimise the likelihood of undergoing such failures. Table 2 gives a summary of a number of such corporate failures, compiled by Fraser and Simkins (2010). The examples illustrate the potential scale of loss that can occur when risk management fails.

Table 1: Entity failures due to poor risk management (adapted from Fraser and Simkins, 2010).

ENTITY	INDUSTRY	CAUSE OF FAILURE	ESTIMATED IMPACT
Enron (USA)	Energy	Financial reporting fraud	USD 3bn
Worldcom (USA)	Telecoms	Financial reporting fraud	USD 9bn
Parmalat (Italy)	Food & Dairy	Financial reporting fraud	USD 5bn
Arthur Anderson (USA)	Accounting/auditing	Corporate governance	Reputational damage & firm collapse
Fannie Mae (USA)	Banking	Corporate governance	USD 10bn & government bailout
Lehman Brothers (USA)	Banking	Inadequate risk management	Bankruptcy

The examples in Table 1 should serve as case studies for entities, and should be analysed specifically by risk practitioners so that the lessons about control failures are harvested. Here, the intention is to avoid similar mistakes, or at the very least, reduce the probability of occurrence.

2.13. Value added by risk management

Risk management as a concept can only be adopted by entities if there is some sort of value to be added. Section 2.9. noted the regulatory requirements for the implementation of risk management. In this instance, the driving force for implementation is to avoid regulatory censure, or worse, the regulatory cessation of

the business operations. This is more a case of protecting value, as opposed to creating value.

In a study undertaken by Le Roux (2016:41), with regard to the development of an ERM implementation model, the following benefits of implementing an effective ERM programme were identified:

- enhanced risk-based decisions;
- reduction of operational surprises and losses; and
- improved resource allocation.

These benefits are closely linked to aspects of managerial activities, and therefore contribute to efficient and effective management practices.

The value that ERM can generate is not only advocated in theory and by academia; the following excerpt from ratings agency Standard & Poor (2007:2) provides evidence of the value attributed to ERM, when executed adequately:

> We now propose to introduce enterprise risk management (ERM) analysis into the corporate credit ratings process globally as a forward-looking, structured framework to evaluate management as a principal component in determining the overall business profile. (The business profile, along with the financial profile, are the key factors of a Standard & Poor's credit rating.) Discussions with company managers, part of our normal credit review process, would inform the ERM evaluation. We would then score companies to benchmark our opinions of ERM quality. Furthermore, we expect that deterioration or improvement in a company's ERM quality would potentially drive rating and outlook changes before the consequences are apparent in published financial results. Companies with superior ERM should have less volatility in earnings and cash flow, and will optimize the risk/return relationship.

Ratings agencies are tasked with assigning risk ratings to entities (commercial entities as well as countries). These ratings indicate the level of risk inherent in interacting with these entities to counterparties.

2.14. Implementing risk management

The preceding sections discussed the requirements of an effective risk management programme, as well as the reasons why such a programme is required. While this sets

a good foundation on which to build a risk management programme, such a programme still requires effective implementation to yield the desired results.

In a study focusing on ERM within the South African insurance industry, it was found that the starting point of implementing a successful ERM programme is the establishment of an ERM culture among employees (Reynecke, 2008:135). Another key recommendation put forth by Reynecke (2008:139) is that the risk management programme must be standardised and driven centrally, as opposed to allowing for each of the various business units to implement their own ERM programmes.

Research conducted on the development of an enterprise risk management implementation model by Le Roux (2016:49) also noted culture as the biggest impediment to implementing an effective risk management programme. This supports the findings of Reynecke (2008:135) that culture is the critical component of ERM success.

Padayachee (2016:38) defines risk culture as “the way in which groups of people use risk management principles when making decisions on uncertain future events…”. The definition encapsulates the common way risk is viewed, understood, and treated within an entity – a shared view. Such a commonality can be driven by the development and implementation of standard risk policies, frameworks, processes, and tools according to the guidelines set out by Smith (2012:3). This does not, however, preclude the necessity for senior management to advocate and display the culture, much like any other change implementations in an entity.

In research about risk management within South African SMEs, Smit (2012:3) identifies the lack of a structured approach as a major barrier to the realisation of an effective risk management programme. The approach advocated by Smit (2012:3) comprises the following three components:

1. Risk consciousness that continuously identifies threats to organisational objectives. This reinforces the findings that define risk management in the context of the management of organisational objectives.
2. Establishing a risk management process that outlines the various steps in undertaking risk management. This is covered in section 2.7, which explores the generic steps in a risk management process.

3. A risk management framework that assists risk owners in evaluating risks. This provides the detailed guidance for identifying, assessing, monitoring, and reporting the risk.

Risk management cannot be seen as a once-off exercise which is implemented and left to run autonomously. The process is ongoing, and since risks are dynamic, the success of a risk management programme depends on it being driven continuously. With technological advancement and globalisation, businesses continually face new challenges. A weakness was identified in an exhaustive case study conducted by Arena, Arnaboldi and Azzone (2010:7). The study focused on risk management within three Italian entities and revealed that in one of the entities, the risk management momentum (in the form of interaction and workshops) dropped significantly after the first year, becoming what is essentially a tick-box exercise on an annual basis to be able to produce annual reports. Risk management that is undertaken as a tick-box exercise will not achieve the intended results, since the underlying activities will be done superficially, instead of with the required vigour. In this instance, the risk management function will have a key role to play in maintaining the momentum and ensuring that buy-in from senior management remains in place.

2.15. Conclusion

There are numerous studies that investigate the link between risk management and organisational performance, but the research has not resulted in a clear verdict. However, newly completed studies based on Standard & Poor's risk management rating and firm performance, have found a positive relationship between enhancing the risk management function and firm value (McShane, 2011). The difficulty in arriving at such a conclusion may be due to varying levels of risk management implemented, whereby an entity with an adequately structured function is able to see a positive link to performance, but an entity with a poorly designed function does not see such a relationship.

The risk management process, as documented in a number of standards, guidelines, and codes, is a pragmatic sequence of interrelated activities that −if followed correctly and applied rigorously − should contribute to a higher probability of achieving organisational objectives. Thus, risk management is integrated with business management, and the two concepts should be viewed as complementary.

The size of the financial services sector and its contribution to GDP, employment, and secondary industries illustrates the importance of efficient and effective risk management within this sector, in order to guarantee the long-term sustainability of sector entrants.

CHAPTER 3: RESEARCH METHODOLOGY

3.1. Introduction

“Failing to plan is planning to fail.” – Benjamin Franklin

This adage is simple, yet salient. When undertaking an activity that must achieve a specific objective, planning is one of the ways to improve the probability of the realisation of positive results. Planning may be undertaken in many forms, and for the purpose of this study, planning takes the form of a research methodology. The research methodology is essentially a determination of the best manner in which to undertake the research project, so that results are achieved, while ensuring accuracy, reliability, and completeness. This chapter outlines the processes employed to conduct the research; primarily the generation of empirical data to address the research objectives.

3.2. Research questions and research objectives

The primary research objective is to determine the most pervasive barriers that prevent risk management from delivering intended results from the viewpoint of risk management practitioners. The research questions relating to the primary research objective are as follows:

- To determine which factors impede the successful implementation of risk management. These will take the following factors into account:
    - personnel factors;
    - organisational culture;
    - economic factors; and
    - factors related to skills, knowledge, and training.

3.3. Research design

A qualitative research design was selected, with the aim to answer the main research question through the exploration of the research topic. Qualitative research was deemed appropriate because, as Reinecke et al. (2016:1) note, the strength of qualitative research is theory elaboration, rather than theory testing, and this study

aims to contribute to the existing body of theoretical knowledge. The interview questions were developed in order to achieve the research objectives.

3.4. Data collection

Data collection represents one of the critical components of any study. The method selected was to conduct interviews with the predetermined participants, and this was determined to be the most suitable approach for the following reasons:

- previous studies that used electronic surveys yielded low response rates in general;
- interviews allow for clarification of any misunderstandings; and
- responses are not as delayed as with qualitative electronic surveys, where the respondents may not have set aside a specific time period to complete the survey.

3.4.1. Population

The primary subject of the study is risk management, even though the study is concerned with identifying barriers to implementing risk management. This being the case, it is postulated that those who are most often exposed to the concept of risk management will be the best source of input for the empirical data. Consequently, risk practitioners were identified as the population set for the study.

While risk practitioners are responsible for the facilitation and coordination of risk management (line management is responsible for the actual risk management activities, according to the three-lines-of-defence model discussed in section 2.7.), the experience in general is that the risk practitioner is regarded as the custodian of the risk management programme.

3.4.2. Sample

The sampling method selected is a hybrid, non-random probability sampling approach. It comprises elements of convenience sampling and stratified sampling. Convenience sampling is also referred to as opportunity sampling and is based on identifying a sample that makes the empirical component of the study easier (Alvi, 2016:29). Stratified samples are selected by identifying subsets of the population based on similarities or common characteristics (Alvi, 2016:20). In the case of this study, the

stratification is according to the job role: that of the risk practitioner. Sampling is necessary for reasons of practicality – it is highly unlikely that responses can be achieved from the entire population due to cost and time constraints. Sampling seeks to identify a subset of the population that will adequately represent (in general terms) the characteristics of the full population.

The sample was identified as risk practitioners that are employed or have been employed in the financial services industry (mostly via LinkedIn, networks built up through IRMSA, and previous working experience). This non-probability approach was employed to counter the risk of non-response or unwillingness to participate. The lack of randomised sampling does introduce disadvantages, such as a higher probability of sample bias. However, for the purpose of exploratory research, the guidance from Alvi (2016:14) indicates that the method selected is adequate for this study. The guidance notes that non-probability sampling is suited to exploratory research for new ideas to be generated, that will be tested systematically later. This is further made clear in the areas for further research as well as Chapter 4 conclusion.

The study was limited to the South African financial services industry; participants were therefore selected from South African entities. The sample size was determined by considering the sample sizes utilised by other researchers that have either undertaken similar research, utilised similar research methods or researched comparable sectors. In so doing, the researcher identified a sample size of 19 being deemed adequate for a study on Enterprise Risk Management as a business enabler in the City of Johannesburg Metropolitan Municipality (Makoro & Van der Linde, 2008:79). This study was conducted by way of questionnaire.

A further study focusing on Enterprise Risk Management within the South African mining sector (Maier, 2013:4), which conducted the data collection via interviews, had a sample size of seven (7).

The study “Risk Management for African Infrastructure Projects in Practice: Identifying Improvement Areas” (van der Kuijp, 2017:37) also made use of interviews to obtain data from respondents. In this study, 12 interviews were conducted with a specifically identified sample.

Based on the number of respondents identified in the studies noted above, and in consultation with a fellow researcher with extensive experience in qualitative research methods, a sample size of 25 respondents was deemed to be adequate for purposes of this study.

For the purpose of this study, risk practitioners were not limited to a specific managerial level or type of risk – individuals who were responsible for specific or specialist risk functions, such as regulatory risk (compliance) or fraud risk, were deemed eligible to participate in the study. This decision was made in order to achieve more representation, and so that potential differences that may be of value to the study could be noted.

The anonymity of respondents and the entities that they represent was deemed to be critical, given the potential reputational impact of linking responses to a specific entity. Anonymity was also maintained to ensure that responses were as honest as possible, without respondents fearing any reprimand for their opinions. Should a specific study be required of a particular entity, the results of this study could serve as input to guide the research objectives or key themes.

3.4.3. Research instrument

The empirical data was collected through semi-structured face-to-face interviews via Skype. The interviews were based on a structured set of questions, with standard response options and respondents were also asked to motivate their responses. The motivation component did not comprise of specific questions; it only required that the respondents substantiate their responses. This was purposefully done to avoid leading questions or bias from the interviewer, as well as to ensure consistency across all interviews. The use of Skype to conduct interviews was beneficial in ensuring efficiency and better access to respondents.

Due to the number of questions and the requirement to motivate each response, respondents were asked to provide concise responses, so that not too much of their time was used. The interviewer directly transcribed the summarised motivations (provided in data-capturing worksheets). The summarised motivations allowed a more efficient thematic analysis, since only the key concepts were recorded.

Initially, 25 interviews were scheduled, however, one respondent was unable to attend their interview due to other commitments. This was not deemed material, since the researcher noticed a saturation point in the data at about interviews 18 and 19.

3.5. Data analysis

The analysis of the empirical data obtained used descriptive rather than inferential statistics. Improvements have been noted over recent years in qualitative data analysis methods and visibility of processes, however the guidance with regards to how findings are generated from such analysis has been identified as still requiring much work (Ritchie & Lewis, 2013:199). Ritchie and Lewis (2013:61) further go on to caution that whilst secondary data analysis is a valuable source of information to provide insight into the research objectives, limitations surrounding the initial research must be taken into account. These include sampling shortfalls, data quality and the fact that certain components or perspectives which are now relevant may have been deemed irrelevant initially. The importance of correctly analysing primary data collected is evident from such observations.

Descriptive statistics were selected as the approach since the research intended to provide a simplified view of responses received from the sample, without necessarily making inferences (Trochim, 2006). The results are a summary of the responses obtained from the interviews.

3.6. Ethical considerations

Ethical considerations as guided by the NWU Research Ethics application form and the NWU Manual for Postgraduate Studies (NWU, 2010:50) were duly considered in undertaking the research. The study and subject matter did not seek to obtain any sensitive data or data of an emotional nature.

In addition to respondents' anonymity being guaranteed, each respondent was advised that they had the right to withdraw from any question and/or the entire process at any time.

3.7. Conclusion

The research methodology section outlines the broad approach used in the research design, as well as the processes followed to collect data. This ensures transparency, as it points out potential shortcomings of the data obtained, and the results of the analysis. This will enable future research that can supplement this study and add to the existing body of knowledge. Each research methodology has advantages and disadvantages, and these were noted and evaluated against the intended purpose of the study in order to determine the most appropriate approach.

CHAPTER 4: DATA ANALYSIS

4.1. Introduction

“A problem well stated is a problem half-solved.” – Charles Kettering

Empirical data is an important component of research. This is even more applicable in current times, since change is rapid and constant, which could mean that previous findings may be outdated or irrelevant.

The intention of the data analysis section is for the researcher to derive key themes and distil key points from the data.

The full questionnaire, including the cover letter, is attached as an appendix (Annexure A). The interviews were premised on the research objectives, and aimed to derive information that would contribute to answering the primary research question, namely, what are at the main barriers to the successful implementation of a risk management programme in financial services entities?

The following section presents the results derived from analysing the content of the interviews, as well as the most salient findings from these results.

4.2. Demographics

It was at the aim of the researcher to interview a set of respondents that was as diverse as possible with regard to experience, educational background, age, and so on, in order to ensure that a wide range of responses was obtained.

The intention was never to tie back any responses to a particular entity, but rather to generate empirical data from risk practitioners within financial services. Therefore, there is no mention of any entity name or respondent name or title.

Respondents were identified to include the following key risk types:

- regulatory risk;
- fraud risk (sometimes referred to as forensics);
- operational risk;
- enterprise risk (mostly focused on operational risk); and

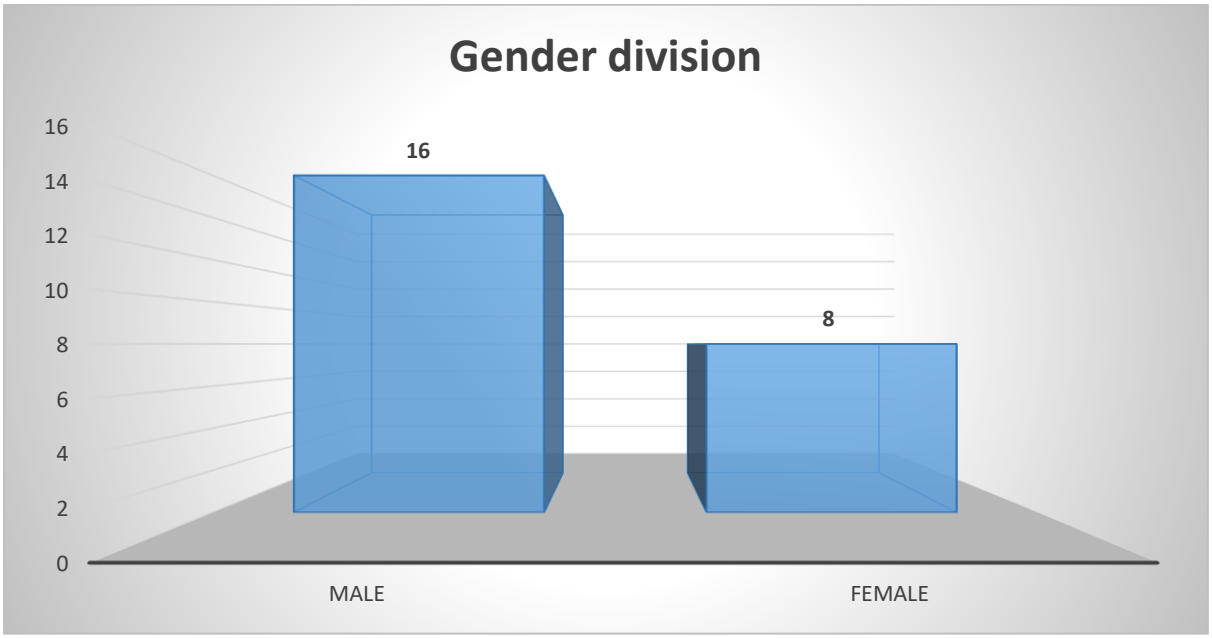
- information technology risk.

The following graphs present visual summaries of the respondent base consulted.

4.2.1. Gender division

The study undertook to obtain input from male and female participants to take into account any gender-specific nuances that may exist.

Figure 4.2.1: Gender division of the sample

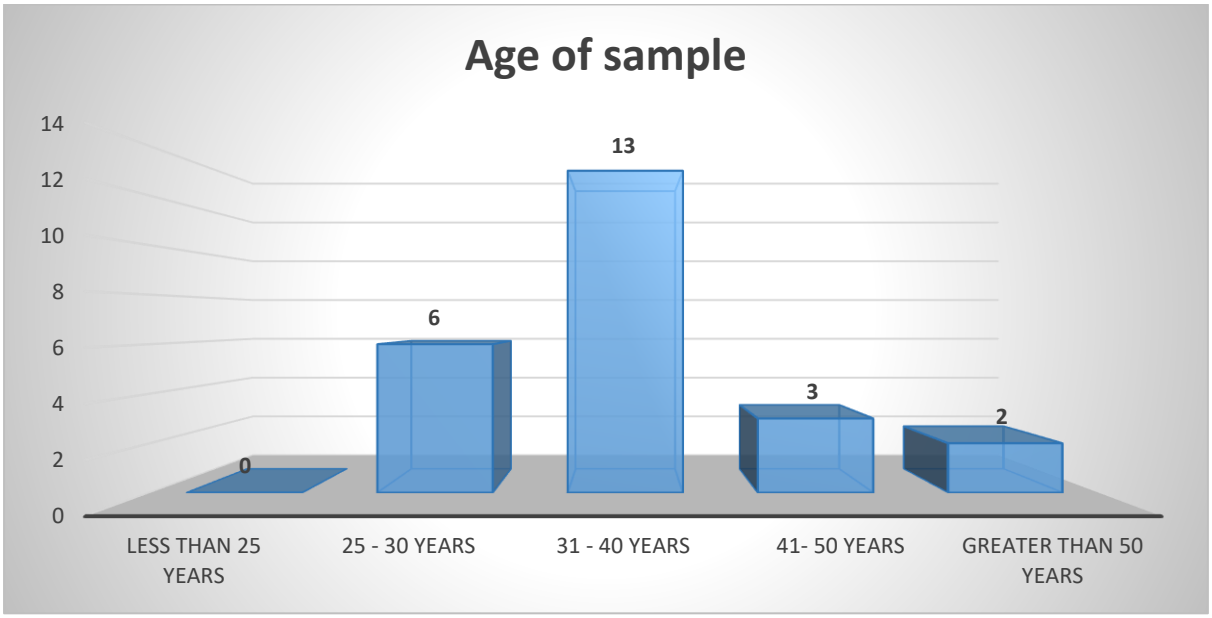


While the respondent base was predominantly male, this did not present any notable nuances in terms of experiences and responses.

4.2.2. Age of sample

The inclusion of age demographics was to portray the breadth of the respondent base, and to obtain the perspectives of different generations.

Figure 4.2.2: Age of sample

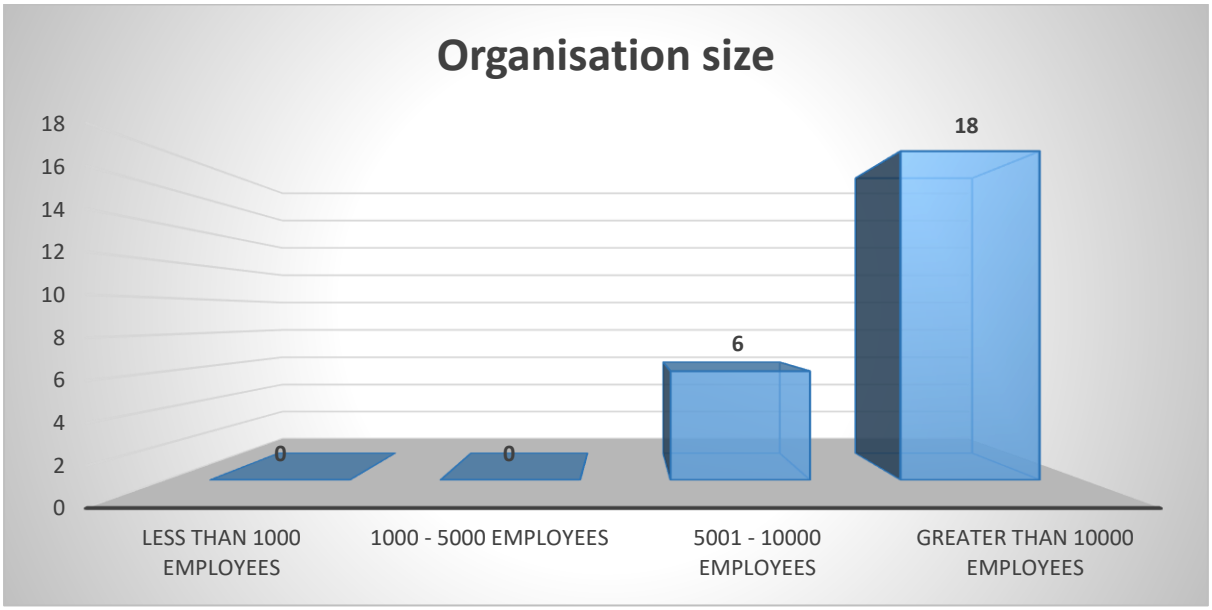


The majority of respondents (54%) were between the ages of 31 and 40. This age group would typically have a number of years of work experience, and be able to contribute valuable insight due to their experiences. As mentioned in the research methodology, the sample was selected so that individuals with experience in the risk environment were consulted – in most instances, experience was closely correlated to age.

4.2.3. Organisation size

The organisation size informs the size of risk management effort. It can be argued that smaller organisations may be able to implement risk management, or make changes to the risk management programme, more easily than larger organisations. Larger organisations, on the other hand, are more likely to have a larger amount of inherent risk, driven by complexity and volume of activity.

Figure 4.2.3: Organisation size



Respondents were all from organisations with an employee headcount of more than 5000 people. The financial services sector employs large numbers of individuals, and the larger organisations (such as the major banks) are some of the biggest employers in the country.

The respondents were from the following employer groups:

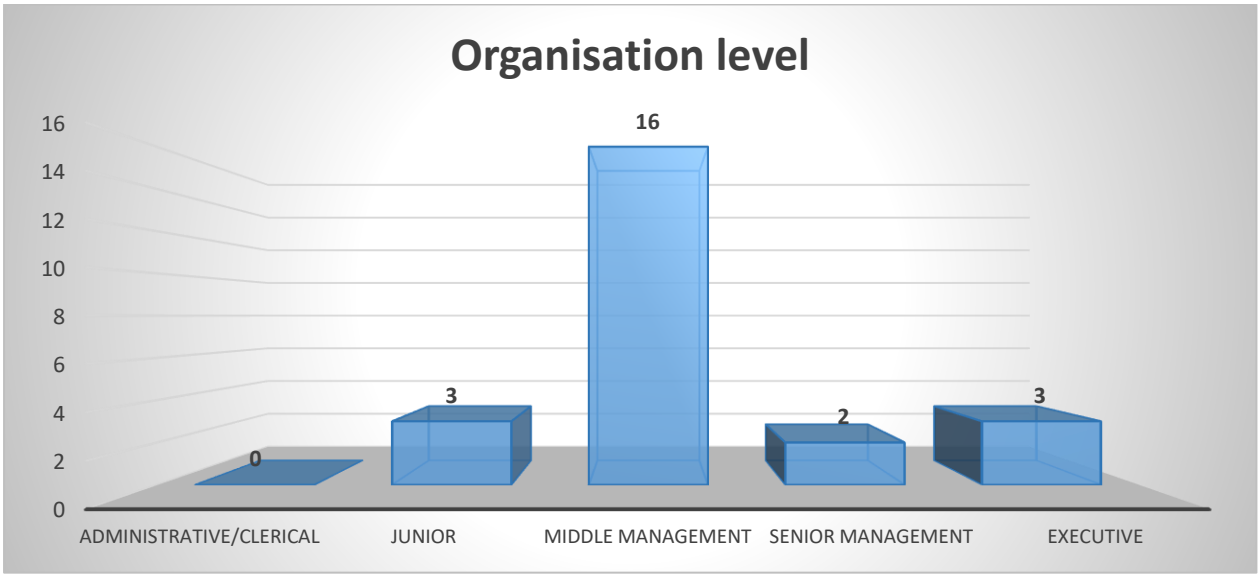
- Two retail banks (ten respondents)
- Two insurers (nine respondents)
- One credit provider (five respondents)

Each of the abovementioned organisations is governed by the Financial Services Conduct Authority (previously the FSB) and have risk management requirements set by the regulator.

4.2.4. Organisational level

Different levels within the organisation are likely to have different risk management experiences, varying from activities at the administrative level, to strategic risk management activities. The responsibilities at the differing levels will also be different.

Figure 4.2.4: Organisational level

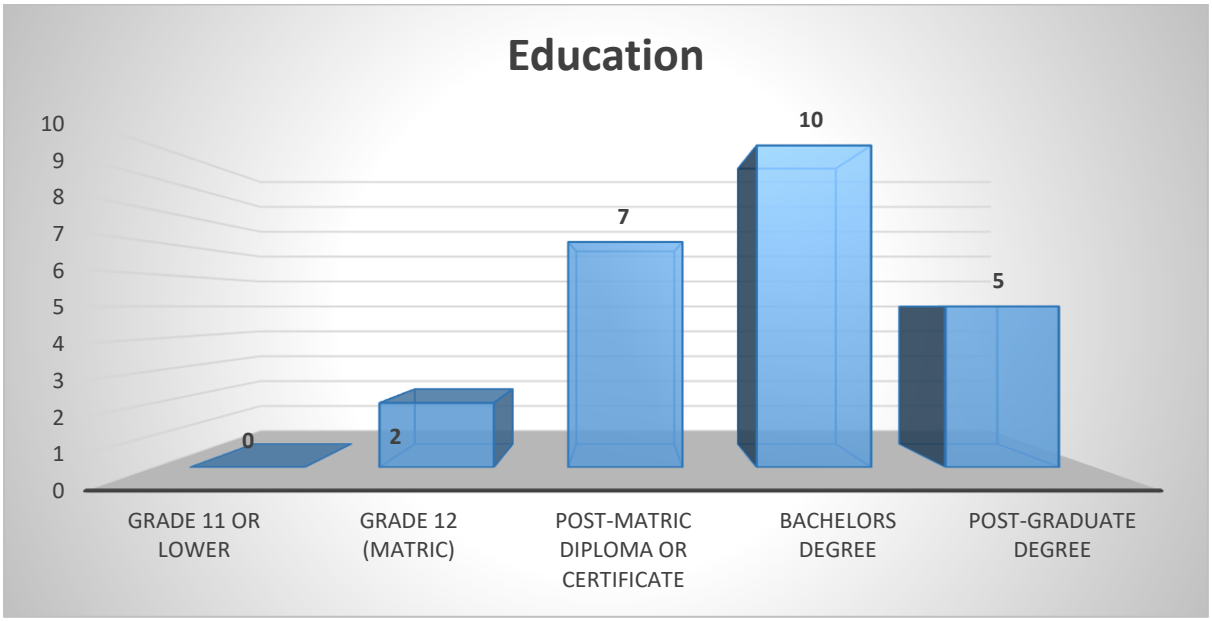


The majority of respondents considered themselves to be in middle management. Certain organisational levels may present business unit middle management, and not necessarily middle management at an entity level. That being said, the importance of risk management is also evident from the above results, because the role of the risk manager (used loosely to refer to the variety of roles that perform risk management) is afforded seniority. Due to the requirement of being able to interact with senior management and executives, the role of risk practitioner should be positioned at the right level to achieve the intended results.

4.2.5. Education

The educational information is presented to determine what educational backgrounds the respondents possess, and the extent to which the risk management function is professionalised. This focuses on formal education rather than experience.

Figure 4.2.5: Education



All respondents have at least Grade 12, or a higher educational qualification: 42 percent of candidates have a Bachelor's degree, and 21 percent have a postgraduate degree. Based on the general job requirements for risk practitioners in the financial services sector, this is not surprising, as candidates are typically required to have a commercially focused degree, or a degree that specialises in IT or Law (in line with the various risk types).

The requirement of a commercially based degree within a financial services organisation relates to the risk management activities that should be undertaken. The risk management practitioner should possess some sort of knowledge of financial concepts to be able to successfully facilitate risk management discussions and/or workshops. The facilitation of the risk management cycle activities, as discussed in Chapter 2, requires commercial acumen, especially where risk identification is concerned. Other responsibilities, such as being accountable for budgets and developing strategy (senior managerial positions), would also require commercial knowledge.

4.2.6. Experience in risk management

It is necessary to determine the number of years of risk management experience that a practitioner has, in order to understand the applicability of responses. The premise of this study is to obtain the perspective of individuals who are or have been involved in implementing risk management. The intention is also to determine whether the varying levels of experience yielded different perspectives.

Figure 4.2.6: Experience in risk management

The majority of respondents (79%) have at least 5 years' experience working in the risk management discipline. The level of experience noted is of such a nature that responses were obtained from individuals who have had experience in establishing, implementing, and/or maintaining risk management efforts.

There was value obtained from less experienced respondents, since their experiences may be more recent and easier to recollect.

From the above graphs, it is evident that a fairly diverse group of respondents was consulted, and therefore the results will provide valuable insight from risk practitioners.

4.3. Responses (non-demographic)

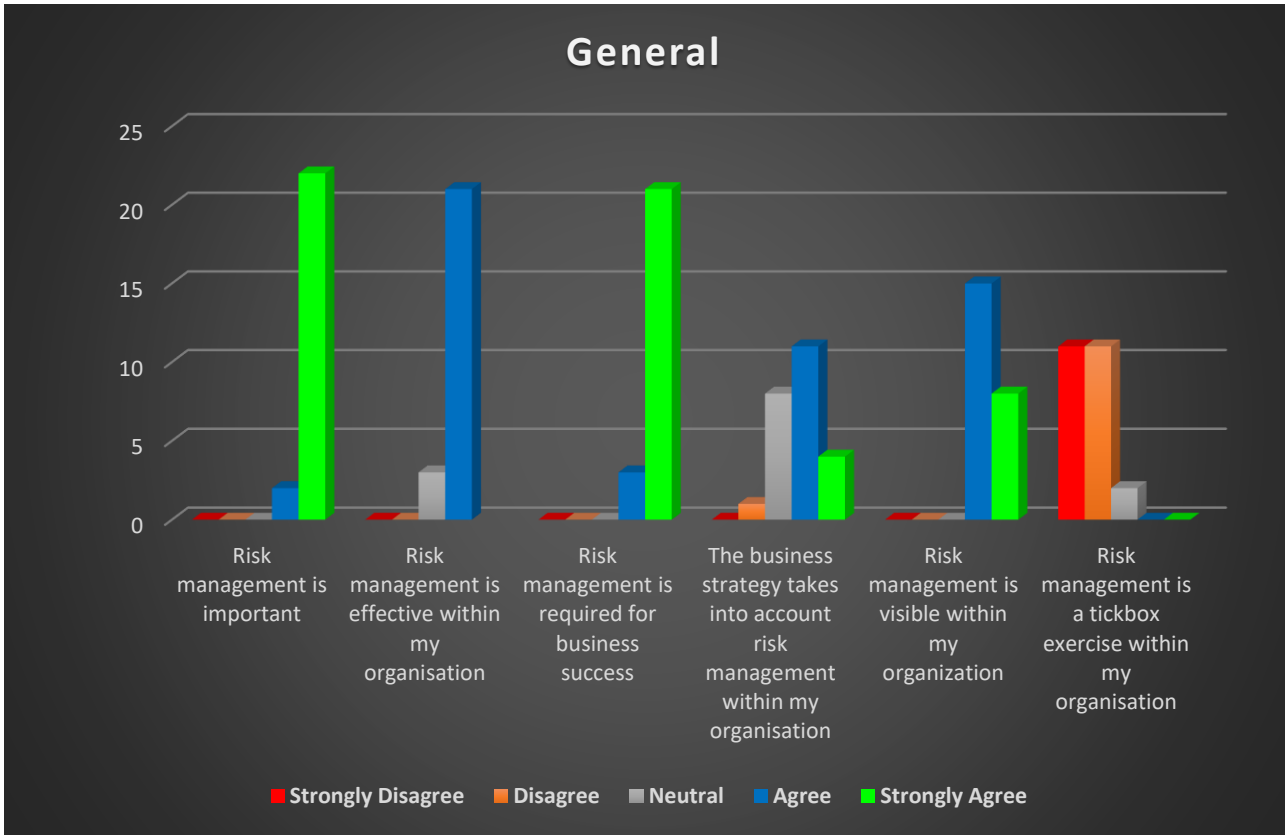
The following section provides an analysis of the responses to each of the items, and a thematic analysis of the results. The detailed question analysis section aims to highlight the key findings that will inform the research topic. The questions were grouped into the following four sections:

1. General
2. Human resources
3. Process management
4. Financial impact

4.3.1. General

The items in this section are general contextual questions that determine the general outlook on risk management, as well as whether risk management is deemed effective or not.

Figure 4.3.1: General responses



The graph in Figure 4.3.1 illustrates several salient points. For the item *"Risk management is important"*, all respondents agreed that risk management is important (92% strongly agreed). Motivations were fairly consistent, and noted the need for risk management to prevent losses or negative incidents, and to help the business achieve its objectives. These motivations correspond closely with the ISO 31000 definition of risk, namely the effect of uncertainty on objectives (SABS, 2009). This is to be expected, since all respondents are risk practitioners and should have an understanding of the need for risk management.

For the next item, *"Risk management is effective in my organisation",* 80 percent of respondents indicated that risk management was effective in their organisations, and this was largely seen to be the case, since no severe incidents or losses were noted. Certain respondents (17%) linked business performance and the fact that the entity is still in existence to the efficacy of risk management. While this is true, it does not take into account sustainability and risk trends (for example, a continually deteriorating risk and control environment is likely to result in significant problems at some point). The remaining 12 percent of neutral responses were essentially undecided, and noted that there are areas that are well managed, as well as areas where improvement is required.

All respondents agreed that for a business to succeed, risk management is a requirement. This validates the responses received for the item *"Risk management is important"*. One of the motivations noted for this statement was *"Risk management is business management"*, which was insightful. Another key theme noted was that risk management was seen to prevent negative outcomes that could hamper business success.

For the item *"The business strategy takes into account risk management within my organisation",* the majority (63%) of respondents confirmed that their organisational strategy considered risks and risk management, while 33 percent of respondents were either unsure whether this was the case or were not exposed to the strategy. This could simply be attributed to the strategy-setting process not being open to many individuals at all levels. A theme noticed was that in considering strategy, risk management would be a consideration to ensure that goals are realised, and that threats to the goals are identified and managed. Senior management respondents

noted that strategy cannot be undertaken without taking risk management into account.

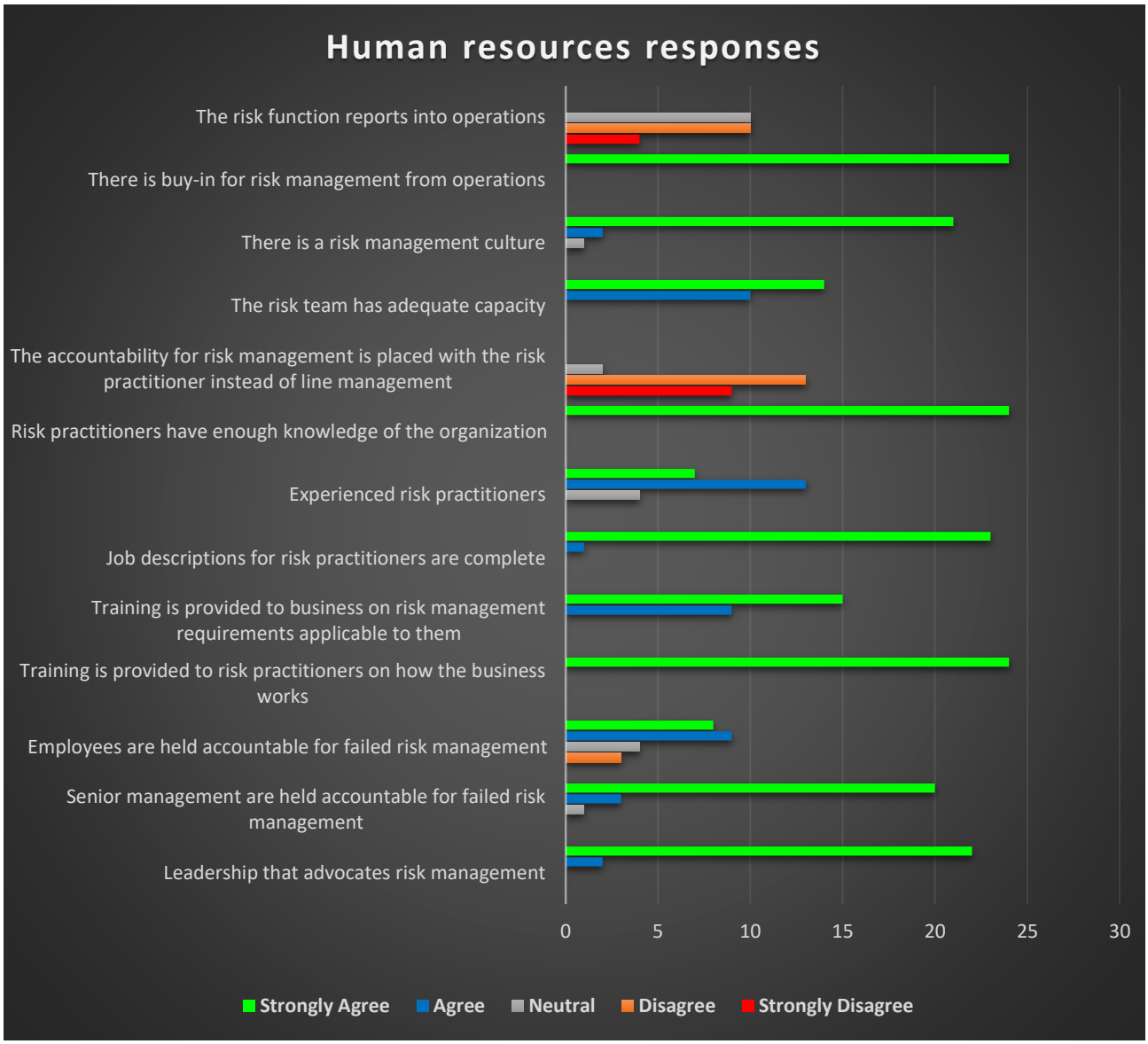
The majority of respondents (63%) agreed that risk management is visible in their organisations, with the remaining 37 percent strongly agreeing. Because the organisations are highly regulated, and risk management requirements in the banking sector are closely monitored by the SARB, it stands to reason that risk management efforts will be visible.

With regard to the last item, *"Risk management is a tick-box exercise within my organisation",* 22 out of 24 respondents disagreed. They considered that risk management efforts are undertaken in earnest in their organisations. Again, with regulatory monitoring and requirements, it would not be as easy to pretend that risk management is in place (but not impossible). The regulatory requirements and supervision was noted as a theme by respondents that made it necessary for risk management to be conducted.

4.3.2. Human resources

This section entails items that pertain to the human element in the organisation, with specific reference to risk management and related requirements. This touches on aspects such as skills, knowledge, training, and culture, to name but a few. Respondents were asked to rate the extent to which each of the statements or scenarios presented in Figure 4.3.2. would contribute to successful risk management.

Figure 4.3.2: Human resources responses



For the first scenario, *"The risk function reports to operations",* 58 percent of respondents believed that the risk function should have an independent reporting line, primarily to allow for non-biased risk identification and reporting. The remaining 42 percent of respondents were neutral, and the main theme here was that risk reporting depends on whether objectivity would be allowed. Respondents noted that risk management would not yield the intended results if objectivity was not allowed to be exercised as part of risk management efforts. This would represent a barrier to risk management.

All respondents agreed strongly with the item *"There is buy-in for risk management from operations".* This is one of the key themes identified. Responses were fairly

similar, and stated that without buy-in, risk management efforts were likely to be in vain. Because risk management is sometimes viewed as a grudge purchase, this makes the need for buy-in all the more important. The motivations for this item mostly entailed the need for the business to support risk management, otherwise the implementation was either going to fail outright, or face severe difficulty.

All respondents agreed that a *risk management culture* would contribute to successful risk management, save for one neutral response.

For the item *"The risk team has adequate capacity",* all respondents agreed that there should be sufficient resources for risk practitioners to perform their required functions. This would be no different from other key functions, but it's confirmation is important to note, especially in situations where there are vacancies that are not filled for long periods of time. The key theme from the motivations was that if there are not enough resources to conduct all the steps within the risk management process, the results will be suboptimal. Regulatory risk practitioners noted that a lack of capacity negatively impacted the effectiveness of compliance monitoring, and ultimately, risk management. Should the risk management function not be allocated sufficient resources, there will likely be challenges. Another theme noted from fraud risk practitioners, was that if the risk function was well staffed, it was more effective.

There was strong disagreement for the item *"The accountability for risk management is placed with the risk practitioner instead of line management",* as 22 of the 24 respondents deemed this to be incorrect, noting that management are accountable as risk owners. This holds true, especially if risks are not regarded as purely negative, and upside risks are also considered. Recent enhancements to risk management standards and literature have featured more content regarding opportunity risk, and no longer focus solely on downside risk. Respondents noted that since risk practitioners do not have authority to make business decisions, placing the risk ownership with them would not lead to effective risk management. Respondents did acknowledge that the accountability for risk management was clear in their respective organisations.

A key theme emerged from the item *"Risk practitioners have enough knowledge of the organisation"*, namely that in order for risk management to be successful, the risk practitioner should have sufficient knowledge of the organisation. While risk

practitioners are not accountable for risk management, they support its implementation and the facilitation of the risk management process (as outlined in Chapter 2). Support and facilitation entails assisting management to develop and embed the required risk management policies, frameworks, processes, and forums. A notable theme was that the support and facilitation of risk management implementation is likely to be more meaningful if the risk management practitioner is able to ask questions that prompt risk identification, correctly inform risk ratings, critically assess controls, or develop key risk indicators. One of the responses noted that when the risk management practitioner has insight of the organisation, frustration is less likely, and there is an improved probability of management buy-in. Another salient point raised from the motivations, is that it is more difficult to fabricate or assess risks incorrectly if the risk practitioner has sufficient knowledge of the organisation.

Experienced risk management practitioners: the outright majority (83%) of respondents deemed experience necessary for risk management to succeed. The remaining 17 percent were neutral, with responses that highlighted that in certain instances, a fresh perspective was perhaps more beneficial than experience, and also that experience is not a guarantee of performance. Respondents noted that for specialist risk types, such as regulatory risk and IT risk, experience contributed to increased effectiveness. A key theme emerging from the subject of experience was that knowledge was the key consideration – thus the previous theme is regarded as significant.

Job descriptions for risk practitioners are complete: 23 of 24 respondents strongly agreed with this item, and the remaining respondent agreed. This serves as the basis for recruiting and assessing performance. The job description serves as the true guide, especially if the line manager is not as helpful as the risk management practitioner needs them to be. Additionally, the job descriptions should adequately distinguish between responsibilities related to the first and second lines of defence. Motivations revolved around the fact that, if the job description was incomplete, the tasks undertaken would most likely not be complete. This was deemed important, but respondents did note that the commonly adopted practices and tasks required by management would, to a large extent, address deficient job descriptions.

Training is provided to business on risk management requirements applicable to them: 38 percent of respondents agreed with this item, and 62 percent agreed strongly. This corresponds with the consensus that management is accountable for risk management, and with the three-lines-of-defence model. If management is accountable for managing risks, they should know all the requirements related to managing risks. This becomes more tangible for risk types such as regulatory risk or fraud risk, where there are specific requirements that must be implemented or adhered to for the risk to be managed within the applicable risk appetite.

Training is provided to risk practitioners on how the business works: all respondents strongly agree that business-specific training for risk practitioners is a requirement for effective risk management. This result is supports the responses to the item *"Risk practitioners have enough knowledge of the organisation".* This is especially true of organisations that offer complex products or services, as undesirable practices could persist for long periods due to the second line of defence not understanding of the underlying risks. The key theme from this question was that in order for risk practitioners to support risk identification, they must know where risks are likely to occur in the processes, and training on business processes, systems, and support functions would enable this. When risk practitioners do not have this information, it is likely to be a barrier to risk management.

Employees are held accountable for failed risk management: 71 percent of respondents were of the opinion that employees should be accountable for risk management failures. This was mostly qualified to note that this was only applicable if the employee had control over the failure, or was responsible for it. From the responses and motivations, this was not identified as a key barrier to risk management.

Senior management is held accountable for failed risk management: the results for this item were more informative compared to responses to the item *"Employees are held accountable for failed risk management"*. From the responses gathered, it is clear that the accountability for risk management resides with management, in line with the three-lines-of-defence model. A total 23 of 24 respondents deemed managerial accountability, and consequences for failed risk management, as a necessity for successful risk management. The motivations indicated that this is a potential material

barrier to risk management success. Essentially, it relates to consequence management: a lack of consequence management may lead to repeated undesirable behaviour.

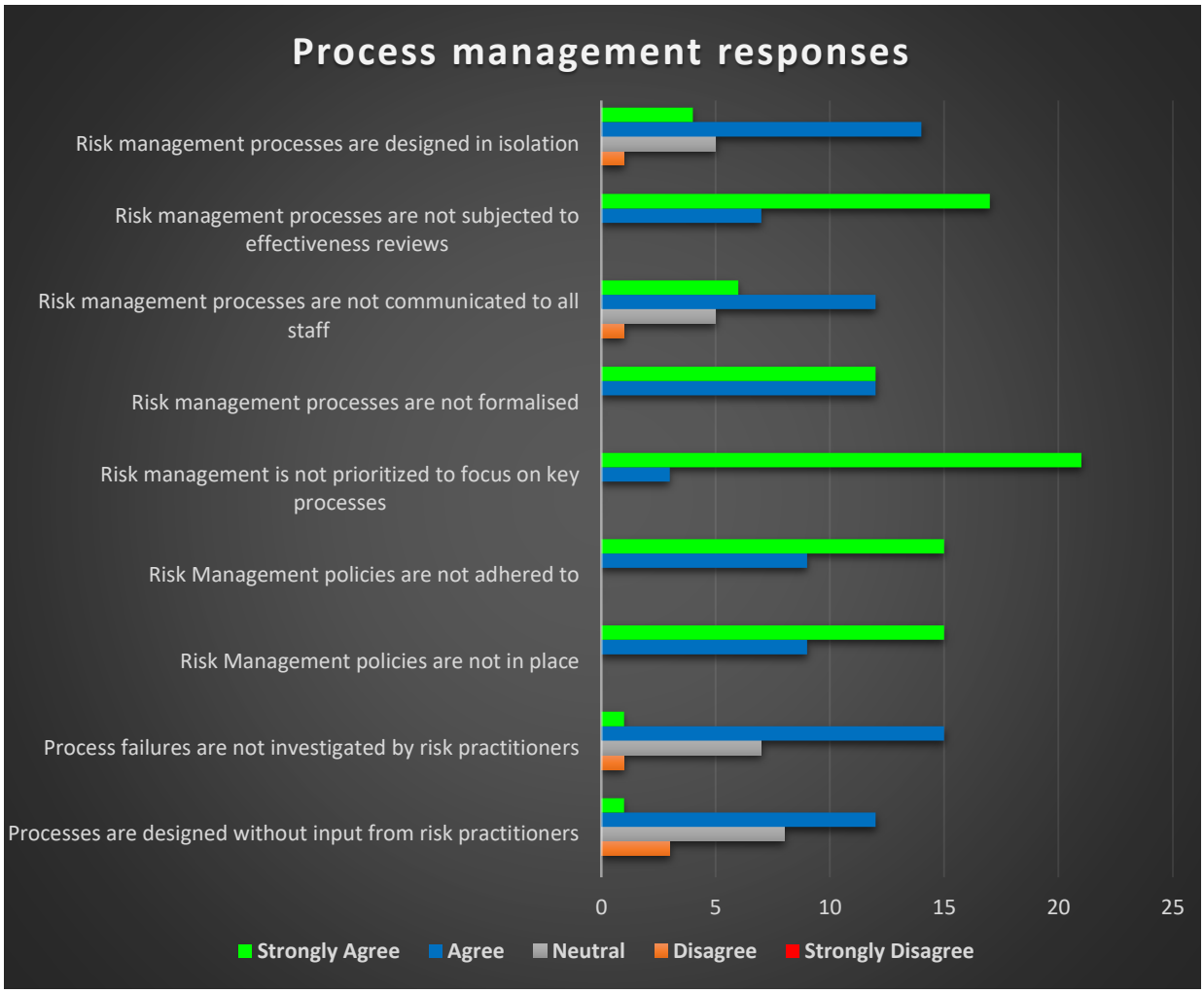
Leadership that advocates risk management: all respondents agreed that this should be a requirement. Organisation leadership determines the focus areas, and if risk management is not deemed important or a key focus area, it is unlikely that efforts to effect risk management will be as effective as they could or should be. Respondents argued that leadership advocacy drives operational buy-in for risk management, which in turn makes the implementation of risk management less cumbersome. A lack of buy-in was identified earlier as one of the key themes that would represent a significant barrier to risk management success, and was echoed by respondents for this question.

A general theme that emerged from the responses was that the quality of risk management depends on the knowledge of risk practitioners, which allows them to engage the business, and identify risks promptly. Respondents placed emphasis on risk identification, noting that it is the starting point of the risk management cycle. An equally prominent theme was that a lack of buy-in from business and senior management was very likely to cause risk management efforts to fail. Because outputs such as risk and control self-assessments are critical risk management tools, buy-in from the business is needed to derive value from these tools. Where buy-in was not achieved, respondents noted that risk management did not receive the necessary time and focus in management committees and executive committees.

4.3.3. Process management responses

The items in this section entail aspects of the day-to-day processes of the organisation, how risk management is incorporated in these processes, and if so, whether it adds value. For this section, respondents were asked to indicate the extent to which each of the statements or scenarios contributed to unsuccessful risk management on the scale provided.

Figure 4.3.3: Process management responses



Risk management processes are designed in isolation: the majority of respondents agreed that this would negatively impact attempts to implement successful risk management. Notably, regulatory risk was noted as one of the risk types where designing processes in isolation was likely to have a major impact. Another common theme that touched on the ineffectiveness of designing processes in isolation, was that the processes designed could be impractical or irrelevant, and the best source to determine this would be operations.

Risk management processes are not subjected to effectiveness reviews: all respondents considered this a contributor to unsuccessful risk management. In fact, 71 percent strongly agreed and 29 percent agreed. Responses mostly entailed the requirement of knowing whether the risk management processes developed are fit for purpose – the effectiveness of risk management is inextricably linked to the effectiveness of the processes developed to drive risk management. Motivations noted

that outdated risk management processes resulted in business not seeing their value, as well as dwindling buy-in for risk management. The general theme was that there should be a measurement of performance if risk management was to maintain its effectiveness, again highlighting that what gets measured, gets done.

Risk management processes are not communicated to all staff: for this item, there were five neutral responses, and one respondent disagreed. The respondent who disagreed, stated that not all risk management processes are relevant to everyone. The remaining respondents agreed that not communicating risk management processes to staff would negatively impact risk management efforts, because staff would not know what is required of them if this is not communicated. The motivations highlighted that while effective communication is important, it is not a key barrier, since the requirements would be known by those responsible.

Risk management processes are not formalised: all respondents deemed the lack of formalised risk management processes to contribute to ineffective risk management. The responses were equally split (50%) between “Agree” and “Strongly Agree”. Without formalised processes, it is unlikely that there is sufficient guidance on what to do and how to do it, which will likely result in inconsistency and confusion.

Risk management is not prioritised to focus on key processes: this scenario forms the most prominent barrier to successful risk management in the process management section − 88 percent of respondents strongly agreed, and the remaining 12 percent agreed. It can be assumed that the key risks would stem from the key processes and activities, and as such, this is where the risk management effort must be expended. Motivations provided by respondents noted that if risk management efforts focused on menial and insignificant processes, it was likely that the significant risks would persist, and the chance of suffering losses would increase. This was identified as a key barrier to risk management effectiveness, not only as a component of the process management section, but in general. Another insightful response received, was that the focus on key processes is critical for functions such as the internal audit when developing their audit plans, otherwise the material weaknesses will not be identified, which will yield poor assurance results.

Risk management policies are not adhered to: as expected, all respondents agreed that this would lead to unsuccessful risk management. This is in alignment with the

responses for *"Risk management processes are not formalised"*, since processes are usually derived from policy provisions and principles. Respondents drew similarities between the importance of risk management policy adherence and adherence to other business policies; they stated that policies provide guidance for correct behaviour.

Risk management policies are not in place: similar to the previous scenario, all the respondents agreed that if risk management policies are not in place, risk management is unlikely to be successful. For risk management policies to be adhered to, there would have to be actual policies available to refer to. Respondents noted that risk management would still be undertaken as part of the day-to-day business activities; however, if policies are not in place, risk management may not be adequately considered at all times.

Process failures are not investigated by risk practitioners: the majority of respondents (63%) were of the opinion that the overall risk management environment could improve if risk practitioners review process failures. Roughly a third (29%) of respondents remained neutral, that is, they did not have a definite view as to whether this would be beneficial or not. This was not deemed a key barrier, but rather more of a value-add activity if it were to take place. Respondents noted that having an independent review of business failures could yield advantages from a different perspective.

Processes are designed without input from risk practitioners: these processes refer to normal day-to-day operational processes. A total of 54 percent of respondents were of the opinion that involving risk practitioners in the design of processes will result in better risk management. About a third (33%) of respondents gave neutral responses, noting that not involving risk practitioners may be inconsequential, and 13 percent disagreed, noting that processes are designed by the subject matter experts who undertake the day-to-day operational activities. From the motivations, this was not identified as a key barrier to risk management effectiveness, although respondents noted that the involvement of risk practitioners had the potential to benefit both them and (potentially) the business.

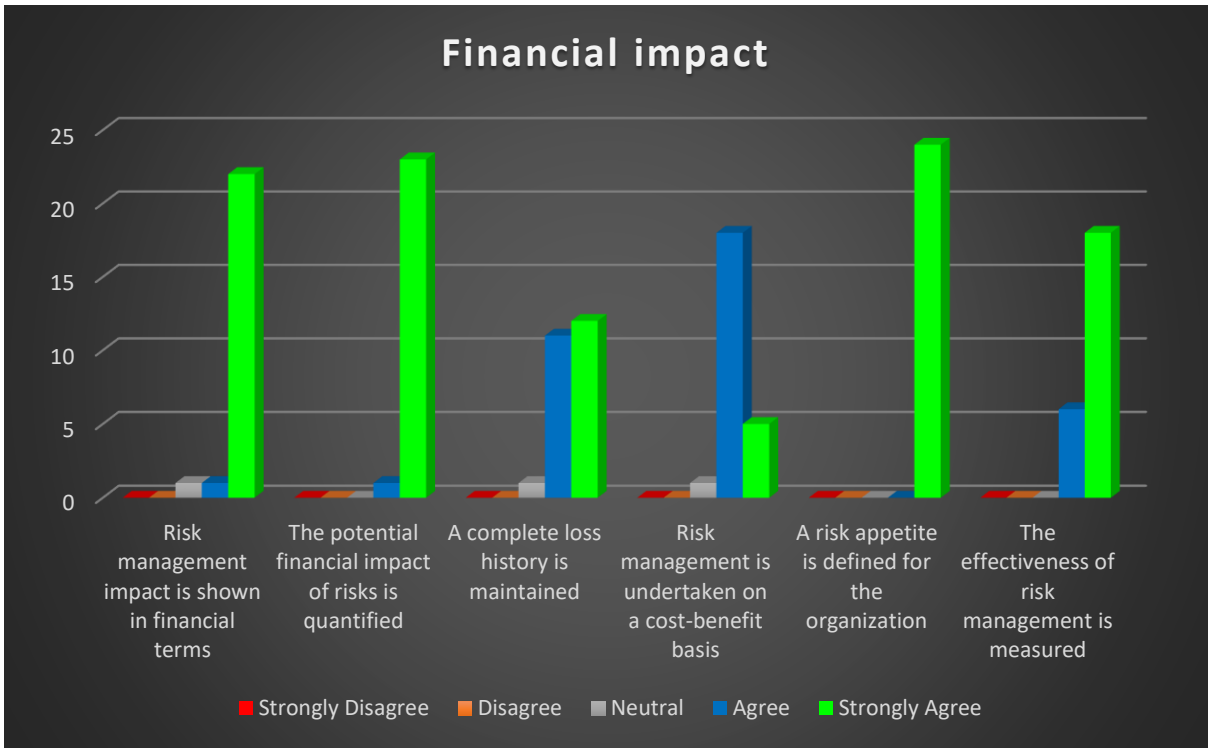
The key barrier identified as part of the process management section, was where risk management was not applied to the material processes in the business. The logic behind this is easy to understand; the key processes (if the analysis is conducted

correctly) are where the key risks are found. Should the efforts not be prioritised to manage the significant risks, risk management effectiveness and efficiency decrease.

4.3.4. Financial impact

The items in this section focused on the financial impact of risk management, and whether expressing the impact of risk management in financial terms enhances risk management. Respondents were asked to rate the extent to which each of the scenarios contributes to successful risk management.

Figure 4.3.4: Financial impact



Risk management impact is shown in financial terms: a total of 22 of 24 respondents strongly agreed that expressing the impact of risk management in financial terms would contribute to successful risk management. This is more than likely linked to buy-in, in being able to show the value of risk management in terms that the business understands. Financial services organisations are for-profit entities, and thus the financial performance is a primary concern – being able to express risk management value in financial terms allows the operation to gauge its importance. Motivations noted that being able to place a monetary value on risk management enhanced the business's focus on risk management, especially if there were potential savings to be realised or losses prevented.

*The potential financial impact of risks are quantified***:** all respondents deemed this to be necessary for successful risk management, with 23 of 24 respondents selecting "Strongly Agree". Similar to *"Risk management impact is shown in financial terms"*, the motivations indicate that the ability to demonstrate what the potential impact of risks are accurately, is likely to attach the requisite focus and resources on risk management. This is probably one of the reasons why areas such as regulatory risk management is a key focus area within the financial services industry, since most legislation specifically notes penalty/fine values that apply for noncompliance. Motivations from regulatory risk practitioners noted that the ability to quantify the potential impact of fines accurately (since they are enacted and known) made the risk assessment and risk treatment processes more meaningful to both the business and the risk function.

A complete loss history is maintained: while this item is noted as an important component of risk management, not many respondents strongly agreed. Loss history is important in financial services entities, as it is a key component for calculating capital adequacy. Respondents noted the value of a loss database as being a good source to identify trends and lessons learnt. A loss history presents insight into some of the risk exposures or potential impacts. This was not deemed a key barrier, but rather an enhancement to risk management maturity.

Risk management is undertaken on a cost-benefit basis: this statement had the smallest number of responses that strongly agreed. Respondents noted that this is a common principle for most facets of the business. This was not identified as a key barrier to risk management; rather, it is a standard business practice that should be employed throughout every business function. The motivations noted that this would be done in any event.

Risk appetite is defined for the organisation: for the financial component, this scenario was identified as the strongest contributor to successful risk management. All 24 respondents indicated that they strongly agreed with this scenario. Risk appetite is deemed important and necessary for risk management success, since it guides how much risk is acceptable. It provides a reference point that allows the business to determine how much risk management is still required. It can be argued that the measurement of risk management success should be within the risk appetite, and

should facilitate the achievement of performance targets. Motivations from respondents noted that this is a new concept that is being implemented and that when it was implemented, it contributed to more meaningful interactions with the business. The interactions with the business are more meaningful, because there is a known reference point that everyone is working towards, which is not subjective. The business is also able to take more risks or accept more risks that fall within the appetite. The motivations indicated that without risk appetite as a reference point, placing descriptors such as “High risk” or “Unacceptable risk” were subjective and debatable.

The salient points noted for the financial section were that, for the business to buy into the process, it is valuable to be able to show the monetary impact of the potential risks (for example, if there is a robbery, how much could the business reasonably lose?). This enables the business to prioritise resources to address the risk, or decide that there is no need to manage the risk further. The key theme that emerged from this section is that the lack of a risk appetite is a barrier to risk management. Risk appetite serves as the reference point for risk management efforts. All risk management efforts should fall within the risk appetite – without the risk appetite, risk management is undertaken based on subjective assessments. The business may assume too much risk or miss opportunities because it is not taking the necessary risks.

4.4. Conclusion

Based on the responses obtained and the motivations supplied, the most pertinent barriers to successful risk management were identified. The methodology used was to identify the responses to the scenarios from the questionnaires that had to highest number of responses that strongly agreed or strongly disagreed. These responses were supplemented with themes formulated from the motivations.

First, it should be noted that there were no material differences in the responses from the different genders. There was, however, an observable difference with regard to the level of experience of the practitioners: the responses of the more seasoned or more senior risk practitioners were more consistent. This is probably due to the fact that the risk management process is iterative. There was also a high degree of similarity between responses. This is to be expected, because there are essentially

two primary risk management standards: the ISO 31000 and the COSO risk framework. The concepts, terminology, and so on are very similar.

Even though the outright majority of respondents indicated that risk management was effective in their organisations, they also noted that this was not the case for all business units, and may not have been the case in the past. This allowed respondents to provide insight into what the barriers to risk management are. More experienced risk practitioners have a greater appreciation of the need to understand the business for successful risk management to take place. Respondents noted that the quality of risk management was better if the risk practitioner knew the business. Certain respondents noted that some of the more successful risk practitioners are operational employees who have moved to a risk management role.

Individuals within the fraud risk environment have a more pronounced appreciation of the value of risk management, since it is more tangible within their space (they experience risks more frequently than practitioners working with a risk type such as strategic risk). Responses from regulatory risk officers were more certain and prudent This can be attributed to the fact that financial services organisations are dependent on licenses, and to retain their license, the organisations must comply with applicable legislation; this leads to a focused intensity on risk management. Regulatory risk officers noted that the potential reputational impacts of regulatory noncompliance were always considered and avoided as far as possible.

The responses indicated that the following 4 scenarios (from a total of 28) are the most pertinent:

1. There is buy-in from risk management from operations (100%).
2. Risk practitioners have enough knowledge of the organisation (100%).
3. Training is provided to risk practitioners on how the business works (100%).
4. A risk appetite is defined for the organisation (100%).

Because items two and three are similar, they were combined into one theme, namely “Risk management practitioner knowledge of the organisation”.

In conclusion, the following key barriers to successful risk management can be formulated from the research:

1. There is no/inadequate buy-in from operations.
2. Risk practitioners have insufficient knowledge of the organisation.
3. There is no risk appetite defined for the organisation.

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS

5.1. Introduction

“In literature and in life we ultimately pursue not conclusions, but beginnings.” – Sam Tanenhaus

This quote rings true for this study in two ways:

1. now that we know what the pertinent barriers to risk management are, we can embark on concerted efforts to counter these threats; and
2. the study has shed light on potential areas of further research, which effectively means starting a new research study.

Chapter 4 identified the most pertinent barriers to successful risk management. The findings are not materially different from findings of previous studies of a similar nature.

5.2. Recommendations

Recommendations for improving the effectiveness of risk management and increasing the probability of effective risk management are given below. They are based on a combination of findings from the literature review, the empirical data, and the researcher’s working experience in the risk management field (mostly in the financial services industry).

Recommendation 1: the entity must have a risk appetite

The entity must determine the amount and types of risks it is willing to take. If no risk appetite is defined, there is no guidance for managing risks, and risk management is done through guesswork. This is the case, since there are no set boundaries, thus it is difficult to determine if the risks in the entity are within its control. The risk appetite must be board approved, formalised, and communicated to management for adoption. Where possible, the risk appetite should include metrics for all risk types inherent in the entity. Entity performance must be measured not only based on financial and operational measures, but should also take into account the performance against risk appetite.

Recommendation 2: obtain buy-in from operations

A lack of buy-in is probably the biggest inhibitor of risk management success, since risk management relies on operations to provide information, develop solutions, and to highlight potential pitfalls, even if this may result in a reprimand in some instances. The lack of buy-in for risk management has been highlighted as an obstacle in other South African studies, and this validates the importance of buy-in.

The methodology for achieving buy-in will depend on the risk maturity and risk culture of the entity. There are three alternatives for developing buy-in for risk management. The first is the inclusion of risk management components into managerial performance scorecards. This could include measures based on risk-loss events, unresolved audit findings, or the quality of risk management reports. The second alternative entails the expression of risks in financial terms. One of the highly rated scenarios was *"The potential financial impact of risk management is quantified"*: 96 percent of respondents strongly agreed that this scenario will contribute to successful risk management. Operational management may buy into risk management if the financial value it adds or protects is clearly visible and quantified. Examples of this are fraud savings (value of fraud prevented) or credit recoveries (value of bad credit recovered). Certain risk impacts, such as reputational damage, are not as tangible; however, there is value in learning from the mistakes of others and highlighting the potential for similar incidents occurring in the entity. The third alternative entails the development of rewards for successful risk management – this may even be in the form of basic awards and not necessarily financial rewards.

Buy-in for risk management must be in place, and in this regard, substance over form is crucial. However, this must be driven from the top, since this is the most efficient manner of doing it.

Recommendation 3: risk practitioner knowledge enhancement

Respondents noted the importance of the risk management practitioner having knowledge of the operation to be able to contribute to effective risk management. The respondents noted that insufficient knowledge of the operation frustrates business, and is less likely to produce an accurate and complete risk profile.

The following are recommendations to ensure that risk practitioners have the requisite knowledge of the business:

- job descriptions or specifications must require input from the business regarding the experience requirements and qualifications;
- risk practitioners must undergo induction for the areas that they support, which should include an understanding of the products and services;
- risk practitioners should have access to all the policies and procedures for the areas they support;
- risk practitioners should be standing invitees to the relevant management committees and steering committees, so that they are up to date with what is happening in the business;
- risk practitioners must have access to any and all training material, such as electronic learning modules;
- risk practitioners must be involved in the development of new products and services, as well as projects (as time permits, prioritised for key projects only); and
- e-learning with content relating to the business processes and organisational information should be made available to risk practitioners.

General recommendations

The following are general recommendations from the literature review as well as from the discussions with respondents:

- the term/title “risk manager” may need to be revisited and replaced with practitioner. The term risk manager is somewhat misleading, as it seems that this role (which is usually a second-line role, not a risk owner) is the one that should be managing the risk;
- there should be clarity in terms of risk management and the process of implementing tools to enable risk management. This clarity should be provided by the risk management function or department;
- all identified, assessed, and reported risks should at all times be linked to a particular strategic objective in order this to contextualise the risk exposure; and

- the effectiveness of risk management must be measured (at least once every two years) and the supporting policies, processes, and tools should be continually reviewed for relevance.

The advent and relevance of Artificial Intelligence (AI) in today's world cannot be ignored by financial services entities without potentially introducing sustainability or existential risks. AI refers to the ability of machines to learn via performing actions, and the learning being continuous. Encyclopaedia Britannica (Copeland, 2019) defines AI as the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings such as the ability to reason, discover meaning, generalize or learn from past experience. The potential uses for and of AI are plentiful, with numerous commentators warning of AI potentially increasing unemployment. This is due to the fact that machines do not really require rest and do not get ill as humans do.

Due to the potential for continuous improvement, enhanced reasoning and the ability to process large amounts of data quickly and accurately the consideration of utilising AI to assist or undertake risk management is a valid one. Within the South African context AI use has already commenced within the areas of Investing, and as at February 2019 there were three AI managed funds within the country from Sanlam Global Investment Solutions, Nmrql and Glacier (Du Preez, 2019). Industry investors note the move internationally (in more developed markets) towards more passive investing with an increased focus on AI capabilities.

Credit Bureau TransUnion already utilises AI in its credit scoring functionality (Credit Vision), and is said to offer improved accuracy and completeness. In its first trial year, a 29 percent decrease in bad debt was noted (Malinga, 2018).

The researcher proposes that risk management practitioners make concerted efforts to stay abreast of AI developments especially with regards to how AI can be utilised to supplement risk management processes. Risk management practitioners should also be highly critical of AI and not blindly rely on the output therefrom without obtaining regular assurance of accuracy, validity and completeness.

The improvement of risk management effectiveness is a journey, and this journey requires constant focus and reinvention. Risk management processes must take into account changes in the operations. This is particularly true in the financial services sector, where change is dynamic. Risk practitioners and senior management will do well not to dwell solely on risks at the operational level; they should also place more emphasis on strategic risk.

First, this study has shown that risk management, while depicted as a simple process (in terms of the risk management cycle), is a complex set of activities that even mature and sophisticated entities sometimes fail to achieve. As a second point, it is consequently important that risk management is afforded the right amount of focus and resources to ensure it achieves its intended function. Last, the intention is to learn from and avoid the mistakes made by other entities where inadequate risk management has caused significant damage or organisational collapse.

5.3. Areas for further research

This study revealed a number of potential areas of further research into the field of risk management. Of interest to the researcher, is studying whether there is a correlation between a robust risk appetite and successful risk management. This may require upfront consensus on what successful risk management is or looks like. A second area of further research would be to determine whether experienced risk practitioners add significantly more value than inexperienced risk practitioners. The researcher deems it worthwhile, as an area for future research, to determine the benefit to risk management gained from embedding AI into operational and/or risk management processes. A final area of research is whether the common risk management tools (key risk indicators and risk control self-assessments) contribute towards successful risk management.

REFERENCES

Accountancy South Africa. 2014. Influence: board members and their role in risk management. https://www.accountancysa.org.za/influence-board-members-and-their-role-in-risk-management/ Date of access: 4 Sept. 2018.

Alvi, M.H. 2016. A manual for selecting sampling techniques in research.

Arena, M. Arnaboldi, M. Azzone, G. 2010. The organizational dynamics of Enterprise Risk Management. Accounting, Organizations and Society, Volume 35, Issue 7.

Bayport Management. 2018. Group risk management framework. Johannesburg: Bayport Management.

Bank for International Settlements. 2010. Overview of the new Basel capital accord.

Bank for International Settlements. 2018. Basel Committee Charter. https://www.bis.org/bcbs/charter.htm Date of access: 15 Jul. 2018.

Centre for the Study of Financial Innovation. 2017. Insurance Banana Skins 2017. The CSFI survey of the risks facing insurers. https://static1.squarespace.com/static/54d620fce4b049bf4cd5be9b/t/592d1ea6bf629a82433f0316/1496129201609/CSFI+Banana+Skins+2017+WEB.pdf Date of access: 28 May 2019

Centre for the Study of Financial Innovation. 2018. Finance for all: Wedded to fintech, for better or worse. A CSFI 'Banana Skins' survey of the risks in financial inclusion. https://static1.squarespace.com/static/54d620fce4b049bf4cd5be9b/t/5b7c1f2d562fa704995d02d7/1534861133477/Banana+Skins_08-18_v5.pdf Date of access: 28 May 2019

Centre of Excellence in Financial Services. 2017. The impact of the 4th industrial revolution on the South African financial services market. https://www.genesis-analytics.com/uploads/downloads/COEFS-TheimpactofthefourthindustrialrevolutiononfinancialservicesinSouthAfrica-final-1-FR.pdf Date of access: 29 May 2019

Chartered Accountants Australia and New Zealand. 2016. Risk management glossary. https://www.irmsa-techlibrary.org.za/#!/module/12/13?component_id=48 Date of access: 31 Aug. 2018.

Chartered Accountants Australia and New Zealand. s.a. Monitor and review. https://www.irmsa-techlibrary.org.za/#!/module/11/478?component_id=48 Date of access: 4 Sep. 2018.

Chapman, R.J. 2006. Simple tools and techniques for enterprise risk management. Sussex: John Wiley and Sons.

Christodoulou, J. 2005. John Dewey: U.S. educator, pragmatist philosopher & psychologist.

CIMA 2006. Paper P3: management accounting risk and control strategy. London: Elsevier.

Copeland, B.J. 2019. Artificial Intelligence. https://www.britannica.com/technology/artificial-intelligence Date of access: 29 May 2019

COSO. 2004. Enterprise risk management – integrated framework executive summary.

COSO. 2017. Enterprise risk management framework: integrating with strategy and performance.

Dewey, J. s.a. John Dewey quotes. https://www.goodreads.com/quotes/7702317-a-problem-well-defined-is-a-problem-half-solved Date of access: 9 Sep. 2018.

Department of Labour: South Africa. 2018. Industrial Action Report 2017. http://www.labour.gov.za/DOL/downloads/documents/annual-reports/industrial-action-annual-report/2017/iar2017.pdf Date of access: 29 May 2019

Dhankar, R.S. & Kumar, R. 2006. Risk-return relationship and effect of diversification on non-market risk: application of market index model in Indian stock market. *Journal of Financial Management & Analysis,* 19(2): 22-31.

Du Preez, L. 2019. In a brave new world, SA investment managers turn to AI to beat the market. https://www.businesslive.co.za/bt/money/2019-02-03-in-a-brave-new-world-sa-investment-managers-turn--to-ai-to-beat-the-market/ Date of access: 29 May 2019

Fraser, J.R.S. & Simkins, B.J. 2010. Enterprise risk management: today's leading research and practices for tomorrow's executives. Hoboken: John Wiley and Sons.

FSB. 2010. FAIS Newsletter volume no. 9. Newsgroup:

FSB. 2014. Board Notice 158 of 2014.

FSB. 2018. FSB Annual report 2017.

FSCA. 2018. FSCA FAIS Notice 54 of 2018.

Garavaglia, B. 2008. The problem with root cause analysis. *Nursing Homes: Long term care management,* 57(2)38-39.

Horev, M. 2009. How to succeed in failure analysis and fail in root-cause analysis. *Electronic Device Failure Analysis,* 11(3):14-19.

Institute of Directors Southern Africa. 2016. King IV Report on Corporate Governance for South Africa 2016. Institute of Directors Southern Africa.

Institute of Directors Southern Africa. 2018. Understanding King IV and what it is intended to achieve. https://www.iodsa.co.za/news/389613/Understanding-King-IV-and-what-it-is-intended-to-achieve.htm Date of access: 30 May 2019

IRM. 2018. A risk practitioner's guide to ISO 31000: 2018.

IRMSA. 2014. The IRMSA guideline to risk management 2014. https://www.irmsa-techlibrary.org.za/#!/module/12/35?component_id=48 Date of access: 4 Aug. 2018.

IRMSA. 2018. IRMSA risk report: South Africa risks 2018. 4th edition. https://www.irmsa-techlibrary.org.za/#!/module/12/501?component_id=48 Date of access: 22 May 2018.

IRMSA. 2019. Get to know IRMSA. https://www.irmsa.org.za/page/About_Us Date of access: 28 May 2019

IRMSA. 2019. IRMSA risk report: South Africa Risks 2019. 5th edition

ISO. 2018. The new ISO 31000 keeps risk management simple. https://www.iso.org/news/ref2263.html Date of acces:26 Jul. 2018.

Kotze, T. 2007. Guidelines on writing a first quantitative academic article.

Lambert, V.A. & Lambert, C.E. 2012. Qualitative descriptive research: an acceptable design.
https://scholar.google.co.za/scholar?q=descriptive+research+design&hl=en&as_sdt=0&as_vis=1&oi=scholart&sa=X&ved=0ahUKEwj6xtmr9qPWAhXJAMAKHdgKBc8QgQMIIjAA Date of access: 14 May 2018.

Laxman, K. 2010. A conceptual framework mapping the application of information search strategies to well and ill-structured problem solving. *Computers & Education,* 55(2)513-526.

Le Roux, H. 2016. Development of an enterprise risk management implementation model and assessment tool (Doctoral thesis). Retrieved from https://repository.nwu.ac.za/bitstream/handle/10394/24950/Le%20Roux_H_Chapter_1_4.pdf?sequence=1&isAllowed=y

Maier, J. 2013. Enterprise Risk Management Implementation: Perceptions of Risk Practitioners in the South African Mining Industry (Master's thesis). Available from https://ujcontent.uj.ac.za/vital/access/manager/Repository/uj:7854

Makoro, L.J. & Van der Linde, T.N. 2008. Enterprise risk management as a business enabler in the city of Johannesburg Metropolitan Municipality (Master's dissertation). University of Johannesburg, Johannesburg.

Malinga, S. 2018. https://www.itweb.co.za/content/DZQ58vVJ9P5vzXy2 Date of access: 29 May 2019

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

National Treasury. 1999. Public Finance Management Act No.1 of 1999. http://www.treasury.gov.za/legislation/pfma/act.pdf Date of access: 29 May 2019

National Treasury. 2009. Public Sector Risk Management Framework. https://oag.treasury.gov.za/Guidelines/Forms/AllItems.aspx?View=%7b1B00811D-F38B-4254-AE4C-0F0D7642653C%7d Date of access: 29 May 2019

National Treasury South Africa.. 2018. New twin peaks regulators established.

NWU. 2010. Manual for Postgraduate Studies.

Okes, D. 2008. The human side of root cause analysis. *Journal for Quality & Participation,* 31(3):20-29.

Oosthuizen, T.F.J. 2007. Management tasks for managerial success. 3rd ed. Roodepoort: Future Vision Business Consultants.

Padayachee, K. 2016. Risk culture assessment of a financial services organisation (Master's thesis). Available from https://repository.nwu.ac.za/bitstream/handle/10394/24946/Padayachee_K.pdf?sequence=1&isAllowed=y

Pillay, V.M. & Zaaiman, H. 2015. Issues with enterprise risk management buy-in: a South African government case study (Master's thesis). Available from https://repository.nwu.ac.za/handle/10394/17107

Reinecke, J., Arnold, D.G. & Palazzo, G. 2016. Qualitative methods in business ethics, corporate responsibility, and sustainability research.

Reynecke, W. N. 2008. Enterprise risk management in the South African insurance industry (Master's thesis). Available from https://repository.nwu.ac.za/bitstream/handle/10394/4215/Reynecke_W.N.pdf?sequence=3&isAllowed=y

RFF Electronics. 2010. Fishbone diagram template. https://www.rff.com/fishbone-template.php Date of access: 4 Mar.2018.

Ritchie, J., Lewis, J. 2013. Qualitative Research Practice. A Guide for Social Science Students and Researchers. http://202.91.10.51:8080/xmlui/bitstream/handle/123456789/3722/Qualitative%20Research%20Practice.pdf?sequence=1&isAllowed=y

SABC News. 2018. SABRIC says 64% increase in cyber-crime. http://www.sabcnews.com/sabcnews/sabric-says-64-increase-in-cyber-crime/ Date of access: 29 May 2019

SABRIC. 2018. Digital Banking Crime Statistics. https://www.sabric.co.za/media-and-news/press-releases/digital-banking-crime-statistics/ Date of access: 29 May 2019

SABS. 2009. ISO guide 73: risk management – vocabulary. https://www.irmsa-techlibrary.org.za/#!/module/12/20?component_id=48 Date of access: 11 Sep. 2018.

Smit, Y. 2012. A structured approach to risk management for South African SMEs (Doctoral thesis). Retrieved from http://etd.cput.ac.za/bitstream/handle/20.500.11838/1726/structured%20approach%20to%20risk%20management%20for%20SA%20SMEs.pdf?sequence=1&isAllowed=y

Smith, C. 2019. Major spike in SA cyber attacks, over 10 000 attempts a day - security company. https://www.fin24.com/Companies/ICT/major-spike-in-sa-cyber-attacks-over-10-000-attempts-a-day-security-company-20190429 Date of access: 30 May 2019

Standard & Poor. 2007. Request for comment: enterprise risk management analysis for credit ratings of nonfinancial companies. https://community.rims.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=fe798de0-fdfd-4f03-a36b-85b24ba2f285 Date of access: 7 Oct. 2018.

StatsSA. 2018. GDP 2018 Q2 Media presentation. http://www.statssa.gov.za/publications/P0441/GDP_2018_Q2_Media_presentation.pdf Date of access: 14 Sept.2018. [Presentation].

South Africa. 1990. Banks Act 94 of 1990.

South Africa. 1999. Public Finance Management Act 1 of 1999.

The Association of Insurance and Risk Managers. 2010. A structured approach to enterprise risk management and the requirements of ISO 31000. https://www.irmsa-techlibrary.org.za/#!/module/12/2?component_id=48 Date of access: 4 Sept. 2018.

The Institute of Internal Auditors. 2013. The three lines of defense in effective risk management and control.

The Institute of Risk Management in Southern Africa. 2018. IRMSA risk report 2018. IRMSA.

Trochim, W.M.K. 2006. Descriptive Statistics. https://socialresearchmethods.net/kb/statdesc.php Date of access: 28 May 2019

Uberoi, R. S., Gupta, G. & Sibal, A. 2004. Root cause analysis in healthcare. *Apollo Medicine,* 4(1)72-75.

van der Kuijp, L.S. 2017. Risk Management for African Infrastructure Projects in Practice: Identifying Improvement Areas (Master's thesis). Available from https://repository.tudelft.nl/islandora/object/uuid:01cf14fa-1730-4710-b0f5-f930416f4894/datastream/OBJ/download

Waterhouse, R. 2015. A day in the life of an enterprise risk management professional. https://www.linkedin.com/pulse/day-life-enterprise-risk-management-professional-rachel-waterhouse/ Date of access: 13 Aug.2018.

Wong, K.C. 2011. Using an Ishikawa diagram as a tool to assist memory and retrieval of relevant medical cases from the medical literature. *Journal of Medical Case Reports,* 5(1)120.

World Economic Forum. 2019. The Fourth Industrial Revolution, by Klaus Schwab. https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab Date of access: 30 May 2019