IT risk management disclosure in the integrated reports of the Top 40 listed companies on the JSE Limited

by

Covanni Hohls-du Preez

LIMITED SCOPE DISSERTATION

Submitted in fulfilment of the requirements for the degree

MASTERS COMMERCII

in

COMPUTER AUDITING

in the

FACULTY OF ECONOMIC AND FINANCIAL SCIENCES

at the

UNIVERSITY OF JOHANNESBURG

Supervisor: Professor Doctor B Marx

October 2016

ABSTRACT

Information Technology (IT) has become an integral part of virtually all modern day organisations. The advent of IT has given rise to numerous benefits which increase productivity and efficiency in the workplace, however, IT also brings with it significant risks that can have an impact on an organisation's ability to function as a going concern. Organisations, especially those listed on the Johannesburg Stock Exchange (JSE), are required to submit an Integrated Report (IR) on an annual basis in which they indicate how they used the resources at their disposal to create value for the organisation and its stakeholders during the year under review. The IR is also a forward-looking document, as opposed to the traditional, backward-looking reports. The purpose of this study is to analyse the Integrated Reports of the Top 40 listed organisations on the JSE and determine the extent to which IT risks are disclosed in their IR and whether the way these risks are managed is also included in the IR as required by the IR Framework. This is done by means of an empirical study consisting of a content analysis of the IRs of the Top 40 listed companies on the JSE. The results of the analysis indicate that more than half of the companies in the sample included IT risk as part of their material risks and outlined appropriate and detailed processes that are followed by the company to manage those IT risks.

KEY WORDS

Risk Management, IT Risk Management, Integrated Reporting, International Integrated Report Committee (IIRC) Framework.

CUT OFF FOR STUDY

All information and documentation used in this study is based on available information up to 30 September 2016. Any corporate governance changes or changes in literature after this date will be incorporated in future research to this study.

TABLE OF CONTENTS

TABLES

FIGURES

CHAPTER 1
INTRODUCTION AND STUDY LAYOUT

1.1 INTRODUCTION

Information Technology (hereafter IT) has become an integral part of modern day business. Fred Smith, Chief Executive Officer of FedEx, emphasised this fact as far back as 2003 when he spoke at a consortium summit about IT, stating that IT was more important than the planes FedEx uses. This can be attributed to the fact that for any transport company, it is imperative to be able to track parcels and thus to be able to charge premiums for fast delivery (Hayes, 2003).

From the beginning of IT in the 1960s, where working on a computer was a specialised task in terms of data processing, to the development of the personal computer in the mid-1990s, much has happened and many advancements have been made in the IT field (Gartenberg, 2006:18). The rapid development of IT in the past years has made it easier for the stakeholders of an organisation to interact with each other while carrying out their business functions. It even allows cross-function collaborations when it comes to product development, marketing and customer services (Tseng, 2008:150).

The biggest development in IT over recent years has been the internet, which in a certain sense, has caused international boundaries between companies to disappear and has created a more 'instant' world. Gartenberg (2006:18) supports this by stating that "we live in a world of multiple devices networked locally and globally and often owned and operated by the end user. Information is shared on and distributed in real time". Sanders (2007:1334) further supports the impact of the internet on the way business is conducted by saying that "of all the IT, the emergence of the internet may have had the greatest impact on information exchange between buyers and sellers".

In order to remain competitive in the modern economy, it is important to ensure prices stay on par with those of competitors and that products are readily available and of good

quality. IT, when implemented correctly, can assist in keeping production costs as low as possible and can differentiate the organisation from its competitors (Rivard, Raymond & Verreault, 2006:30). Effective IT systems which are managed correctly ensure constant communication between the organisation and their supplier. The result of this direct communication is the quick and reliable delivery of products when and where they are needed (Sanders, 2007:1334).

IT did not only have an impact on existing organisations, it also gave rise to completely new businesses such as Amazon.com, which would not be able to survive without the presence of technology (Gartenberg, 2006:18). In Bordeaux, France's Chief Information Officer (CIO) took the importance of IT presence one step further. A system has been developed where tourists can use the SnapScan Application on their smartphones to obtain information on some of the country's major landmarks. All they have to do to obtain the information is scan the code and the information is immediately available on their phones. Codes are even available to give information on any form of public transport when needed (Shinn, 2012:18).

From the discussion above, it is clear that the development of IT over the years has brought a significant amount of benefits to modern day businesses, but with these advances, there came additional risks as well. The next section looks at the additional IT risks companies are faced with.

1.2 INFORMATION TECHNOLOGY RISKS

With IT being such an integral part of modern day business, companies face many new risks. This is emphasised by Marx (2008:82) who is of the opinion that "the development of IT, electronic commerce and increased reliance and dependency on IT resources have exposed modern businesses to many challenges and significant new risks". IT Risks can be defined as "any event or action that could cause a loss or damage to computer hardware, software, data or information" (Wong, 2016). IT Risks can be divided into five main groups. Each of these groups has its own smaller elements and these elements

can sometimes be found in more than one group (Parent & Reich, 2009:142). The five groups identified are:

- IT Competence risk which refers to the IT knowledge of the directors of an organisation;
- IT Infrastructure risk which refers to the risk that computers, networks, operating systems, applications and databases of an organisation do not function as intended;
- IT Project risk which refers to the risk typical of a new and specifically large project being undertaken which is related to IT specifically;
- IT Business Continuity risk which refers to the risk that the organisation is not able to function in the event of a disaster as critical information is lost; and
- IT Information / Security risk which refers to the risk of unauthorised persons gaining access to confidential and sensitive information.

Refer to Annexure A for a more comprehensive discussion of each of the abovementioned risks.

It is important for an organisation to inform current stakeholders and potential investors of some of the additional risks that companies face due to the presence of IT and how those risks can affect the organisation. The next section discusses the importance of risk disclosure in financial statements.

1.3 RISK DISCLOSURE IN THE INTEGRATED REPORT

According to International Accounting Standard 1 (IAS 1) as set by the International Accounting Standards Board (IASB), companies are required to provide annual general purpose financial statements. IAS 1 defines general purpose financial statements as "those intended to meet the needs of users who are not in a position to require an entity to prepare reports tailored to their particular information needs" (IASB, 2011). According to Amran, Che Haat and Manaf Rosli Bin(2008:39), the annual report of an organisation,

which consists of financial and non-financial information, has been the chief means of conveying useful information for investment, credit and other decisions over the years. As will be discussed in Chapter Three, an explanation is given of where the Integrated Report (IR) fits into the complete set of the Financial Statements. In modern day reporting, individual statements such as the Statement of Comprehensive Income and the Statement of Financial Position are not released on their own anymore; the IR has replaced the individual statements with one report, to be issued to all stakeholders, which is aimed at providing stakeholders with a comprehensive view of the organisation. The IR tends to present a more holistic picture of the organisation's strategy, instead of just providing pure financial information. Most organisations have used their annual reports as a basis and have included the elements of an IR, renaming their reports as Annual Integrated Reports. However, through this method of reporting, the page number of reports has increased significantly and there may be the risk that too much information is being imparted at once (de Villiers, Rinaldi & Unerman, 2014:1045).

Risk is a very important part of disclosure, but it is often not done with enough consultation and care. One of the possible reasons for not giving adequate attention to risk disclosure is the fear management has of the possible negative effects this may have on the organisation. This notion is echoed by Deumes (2008:123) who says that "managers may perceive that there is a cost imposed on the organisation by competitors who exploit the information to the detriment of the disclosing organisation".

On the other hand, by disclosing risks, managers can increase the transparency and reliability of the IR. Disparities can also be reduced between management's ability to deliver and what an investor understands (Deumes, 2008:122). Investors will gather as much information as possible on risks before they make an investment decision (Amran *et al*., 2008:42). Clear, readable and understandable disclosure results in stronger reactions from investors, especially small investors. This leads to more positive reactions when there is good news and more negative reactions when there is bad news (Rennekamp, 2012:1343). Proper risk disclosure reduces potential investors' uncertainty in terms of future organisation cash flows (Gao, 2010:3). Sometimes even customers,

staff and other stakeholders benefit from risk disclosure (Miihkinen, 2012:441). Part of risk disclosure is not just to report on the risk, but as stated by Miihkinen, to provide information on how this risk is managed to increase shareholders' wealth and limit the possibility of financial failure (Miihkinen, 2012:441). The management of risk, especially IT Risk Management, is discussed in greater detail in Chapter Two.

From the discussion above, it is evident that organisations ought to disclose their specific risks. The disclosure of risk helps to ensure transparency and provide insight into current investments, it assists stakeholders with decision-making and assists potential investors with investment decisions.

1.4 BACKGROUND TO THE RESEARCH PROBLEM

It is clear that IT is a dominant factor in the modern business world but that it has also brought with it previously unknown risks. IT has had an impact on businesses and audits in an IT environment from as early as the mid 1990's. ISACA (Insformation Systems Audit and Control Association) released a guidance document named COBIT (Control Objectives for Information and Related Technology) in 1996 to assist audit teams auditing in an IT environment. In 1998 the second version was released and in 2000 the third version. COBIT four was release in 2005/7 (Harmer,2012). COBIT five, which is the latest version of COBIT, was released in 2012 and is a comprehensive framework to assist with IT risk management. The importance of IT frameworks are further emphasised by PricewaterhouseCoopers (2009:35) in the following statement:

> "King III recognises that IT has become an integrated part of doing business today, as it is fundamental to the support, sustainability and growth of organisation. IT cuts across all aspects, components and processes in business and is therefore not only an operational enabler for an organisation but an important strategic asset. As well as being a strategic asset to the organisation, IT presents the organisation with significant risks. The strategic assets of IT and its related risks and

constraints should be well governed and controlled to ensure that IT supports the strategic operations of the organisation".

The governance of IT and its related risks only began receiving proper attention when the third King Code of Governance for South Africa was published in 2009 (hereafter King III). King III devotes an entire chapter to IT Governance. In Chapter Four of the Code, it is stated that IT Governance is the responsibility of the Board of Directors (BoD). Although guidance is provided in this chapter on how to ensure effective IT Governance, the BoD still has the option to apply the recommendations or not. If the BoD does not apply the recommendations, the BoD have to disclose and explain why they were not applied (Institute of Directors (IoD), 2011). The difference between King III and the previous King reports is that King III is based on an 'apply or explain' basis rather than a 'comply' basis.

The King IV report on Corporate Governance is due to be released in November 2016 and places even greater emphasis on the importance of IT Governance and not just IT Governance in general, but specifically IT Security Governance. It provides detailed guidance on best practice for governing IT risk (IoD, 2016:18). These recommendations and the governance of IT is discussed in greater detail in Chapter Two.

Even though the recommendations put forward in King III were simple and easy to put into practice, boards are still struggling with the implementation of IT Governance (EY, 2006). The board struggles to fully understand IT and its potential risks. It appears that boards are also failing to understand the value that IT can bring to the organisation, mainly because they do not understand IT language or how IT can add value to the organisation. This lack of understanding makes IT Governance a daunting task for the BoD (EY, 2006:2). This is further emphasised by McKinsey & Company when saying boards have to learn a second language – one that is focused on digital products and platforms (McKinsey & Company: 2016). The reluctance of boards to embrace IT and give it the necessary attention is echoed by Valentine and Stewart (2013:350) who note that "any lack of skilled attention to technology by boards may occur because directors do not

understand the relationship between business use of information and company success". IT does not receive enough attention during board meetings and pressing issues are thus not discussed. More often than not, IT only gets a slot on the agenda when funding is required for a new project (EY, 2006:3). Valentine and Stewart (2013:346) further state that "industry research shows that board level willingness to rectify the gap between awareness and action is low or non-existent", which makes it difficult to align business with IT if there is no commitment from management.

In a study conducted by PricewaterhouseCoopers (2006:17), three broad categories were identified that lead to such difficulties with IT governance:

- Culture:

  Often, there is a difference in culture between the IT department of an organisation and its operational side. These two parts of an organisation do not always agree on things.

- Resistance to change:

  Most people are afraid of change and will try to keep things around them as familiar and consistent as possible.

- Lack of proper communication:

  Proper communication is very important in an organisation. When clear communication is not provided to employees, a feeling of fear and uncertainty of the future may arise.

In order to obtain support and buy-in for IT projects, it is important that the CIO is able to explain the project in a manner which can be readily understood by the Chief Executive Officer (CEO) and other board members (Mercury Business Technology Optimisation, 2005:4). If the CIO is not actively involved at board level, there is the risk that the CEO will not be able to provide high quality reports due to a lack of knowledge (Valentine &

Stewart, 2013:351). From the above it appears that the board do not fully understand IT, and it has been the situation for some time. McKinsey & Company(2016) are also of the opinion that boards do not fully understand IT and its purpose in the company when saying in their quarterly report that more directors feel outmatched by the ferocity of changing technology The purpose of this study is to determine to what extent IT risks and IT Risk Management are being disclosed in the Integrated Report (IR) of organisations in terms of the IR Framework.

1.5 STATED RESEARCH PROBLEM

It can be argued that companies rely greatly on IT to remain competitive and consequently, they must be able to effectively address the additional risks associated with IT. This is emphasized by Drnevich and Croson (2013:483) when saying that companies rely greatly on Information technology for business success as it directly affect the mechanisms through which value is created and captured to earn a profit. To ensure the transparency of information for all the stakeholders in an organisation, it is important for management to identify the relevant risks, especially those relating to IT, and to manage and disclose them properly. It is therefore vital that management understands its business, its dependence on IT, how to manage the risks and how to properly inform stakeholders of these risks. The stated research problem can therefore be determined as:

> *"An investigation of the extent to which IT risks and IT Risk Management are currently disclosed in the Integrated Reports of the Top 40 listed companies on the Johannesburg Stock Exchange."*

Literature to further support the research problem can be found in King IV where the Institute of Directors (IoD) recognises that information technology is changing at a rapid pace and has a significant impact on the way business is conducted. Therefore, a specific section has been added to the Code to ensure management is aware and able to analyse complex and often hidden interdependencies in order to build resilience thereto. One of

the principles built into the Code to address such additional IT risks indicates that "the governing body should govern technology and information in a way that supports the organisation in defining its core purpose and to set and achieve strategic objectives" (IoD, 2016:53).

The view of Wessels (2006:131), who is of the opinion that "South African business organisations operate in an environment that is changing rapidly, and where one of the key drivers of this change is IT", is further supported by the IoD (2011) in the statement: "IT has become pervasive because it is an integral part of the business and is fundamental to support, sustain and grow the business" (IoD, 2011:82). Atyam (2010:343) and Ko and Dorantes (2006:13) also emphasise the importance of IT and the change in business that came when they state that with "today's businesses being IT enabled, the complexity of risks affecting the business has increased manifold and the need to gauge the IT risks acting on the business operations has become paramount". They add that "as the number of organisations that conduct their business electronically grows continuously, information security becomes one of the major concerns for top management". Scott, (2015) is also of the opinion that IT has an important role to play in the workplace of today and believes that IT allows businesses to expand quickly and reliably. IT has also assisted in removing workplace boundaries with the introduction of video conferencing, social networks and virtual office technologies (Scott, 2015).

Stated research problem:

An investigation of the extent to which IT risks and IT Risk Management are currently disclosed in the Integrated Reports of the Top 40 listed companies on the Johannesburg Stock Exchange.

1.6 STUDY LAYOUT

The study is divided into the following chapters:

Chapter 1: Introduction and study layout

In this chapter, the background to the study and an explanation of the research problem are provided. The background focuses on the importance of IT in modern day business and the IT risks faced by organisations. The objective of this chapter is to provide the reader with the background of the study as well as the outline of the rest of the study.

Chapter 2: Obtaining an understanding of IT Risk Management and the need for disclosure

Chapter Two discusses the concept of Risk Management with particular reference to the management of IT risk. Further to the requirements of King III, the requirements of King IV are discussed with regard to IT Governance. The objective of this chapter is to obtain an understanding as to what IT Risk Management is and how it is governed by the King Code.

Chapter 3: The concept of Integrated Reporting

This chapter examines the purpose of Integrated Reporting and risk disclosure requirements. The chapter also focuses on how Integrated Reports have evolved over the years and what benefits Integrated Reports can provide to the organisation and shareholders. The objective that is aimed to be achieved is to obtain an understanding on what Integrated Reporting is and how risks, IT risks, should be disclosed in the report in terms of the IR Framework.

Chapter 4: Empirical study and research findings

Based on the literature study, a content analysis is conducted to determine whether companies comply with the relevant disclosure requirements as per the IR. The methodology adopted in the study as well as the research findings are also discussed. The aim of this chapter is to provide detail on the research performed on the IR from the Top 40 listed companies on the Johannesburg Stock Exchange (JSE).

Chapter 5: Conclusion

In this chapter conclusions are drawn from the literature study and the research conducted. Recommendations are made and areas for possible further research are identified. The objective of this chapter is to provide an overall conclusion on the findings as per the individual chapter objectives.

1.7 CONCLUSION

Chapter One discussed the importance of IT for modern day businesses and the fact that companies have reached a stage where the majority of them cannot function effectively without some form of IT present. The concept and importance of risk disclosure was also discussed.

The literature review clearly indicated that most companies' boards are not as well informed about IT as one would like them to be. It also indicated that there is a need for research on whether IT risk receives the same attention in terms of disclosure as other operational risks within the organisation.

The next chapter examines IT Risk Management and how it should be managed in terms of the relevant codes and standards.

CHAPTER 2
IT RISK MANAGEMENT AND THE NEED FOR DISCLOSURE

2.1 INTRODUCTION

Risks are an important part of an organisation's business activities. This is evidenced in the fact that it is mandatory in certain industries such as the banking sector to have a Risk Management system in force (Ecker-Lala, 2010:218). Attributed to globalisation and the increased connectivity of organisations, risks are evolving at a rapid pace. Change, including IT developments, is taking place at a fast pace, requiring Risk Management to adapt to what is termed the 'new normal' (IoD, 2016:18). Nocco and Stulz (2006:8) place further emphasis on the fact that organisations need to take note of changes in how business is conducted. They are of the opinion that the changes that have occurred over the past few years in the way business is conducted, coupled with the continuous reliance which is placed on IT networks, have brought about a significant shift in the Risk Management role of an organisation. Sarrazin and Willmott (2016) echoes the importance of a different and continuous Risk Management approach due to the presence of IT in the modern day business as cyberthreats is a continual threat and all controls might not always be able to address hacker incursions. It is also mentioned that downtime of a system need to be managed as a real risk to ensure customer confidence is not eroded.

Effective Risk Management and proper Risk Management procedures to monitor risks in a consolidated manner give an organisation a competitive edge over one which assesses and monitors risks on an individual basis (Nocco & Stulz, 2006:8). This is further emphasised by Adeusi, Akeke, Adebisi and Oladunjoye (2014:339) when saying that banks who implement effective risk management processes obtain advantages such as increase in reputation and ability to create more customers and increase efficiency and profitability. Effective Risk Management enables an organisation to take more strategic business risks and use opportunities relating to its core business for the benefit of the organisation (Nocco& Stulz, 2006:9). One of management's essential roles in an

organisation is to manage risk. In order to ensure the negative impact of risks on an organisation is eliminated or at least kept to a minimum, possible risks that can be encountered during the course of business have to be identified at an early stage and managed with the correct level of skill (Ahmed, Capretz, Sandhu & Raza, 2014:280).

The importance of Risk Management for an organisation is therefore evident. The next section firstly defines and discusses Risk Management in general as well as the shareholder value and competitive advantage that can be gained when effective Risk Management procedures are implemented in an organisation. Secondly, IT Risk Management is examined, followed by a discussion of the specific recommendations for IT Governance in terms of the King IV Report on Corporate Governance. King IV is only applicable from 1 April 2017, thus the IR analysed will not be in line with King IV recommended practices. The recommended practices, however, are similar to the recommendations of King III and therefore the discussion on King IV is deemed appropriate. The recommendations of King III on IT Governance include, but is not limited to:

- The responsibility of IT Governance is that of the board (IoD 2011:39);
- IT should be aligned with the sustainability and performance objectives of the organisation (IoD 2011:40);
- The responsibility of implementation should be delegated to management (IoD 2011:40);
- Significant IT investments and expenditure should be monitored by the board (IoD 2011:40); and
- Board should ensure IT assets are managed effectively (IoD 2011:41).

2.2 RISK MANAGEMENT

2.2.1 Definition of Risk Management

Risk Management can be defined as “a set of principles and practices aimed at identifying, analysing and handling risk factors to improve the chances of achieving a

successful project outcome and/or avoid project failure" (Bannerman, 2008:2120). Nikolić & Ružić-Dimitrijević (2009:595) agree with the abovementioned definition when they say that Risk Management involves analysis, planning, implementation, control and monitoring of implemented measurements and risk assessment. Another perspective to view Risk Management is that of Elahi (2013:120) who notes that, "Risk Management is what we do to shape or be prepared for the uncertain future. While we cannot accurately predict a particular future by focusing on a range of alternatives, we can better prepare for uncertainty or even embrace it".

The Risk Management process consist of three main steps, namely, Risk Identification, Risk Analysis, Risk Evaluation / Mitigation. Each of the three steps is discussed individually below.

Risk Identification

The first step of Risk Management forms the basis on which Risk Management is based. In this step, all risks that can potentially exist needs to be identified. The risks can stem from internal or external sources. They are also not limited to only a certain project or part of the organisation, but are added to the risk list as they are identified (Toader, Brad, Radac & Marin, 2010:455)(Crain, 2014).

Risk Analysis

After all the risks have been identified, it is important that they are analysed (evaluated). The evaluation of risks is important in order to determine the potential impact they might have on the organisation, should they be realised. The evaluation of risks is a complicated process and cannot be taken lightly (Toader *et al*., 2010:456)(Crain, 2014).

Risk Mitigation

The last step in the Risk Management process requires management to implement controls or measures which address the risks that have been identified appropriately. Preferably, these controls or measures must be known to management and they need

to ensure that by applying these measures, additional risks will not be created (Toader *et al*, 2010:456)(Crain, 2014). Some of the strategies available to management to mitigate risks include:

- Acceptance, when management is aware of the reduced risks and is willing to continue without reducing the risks further or eliminating them;
- Avoidance, when there are some unexpected changes to a plan or decision and management decides to avoid the risks, even if it means that the project will be lost;
- Monitoring and establishment, when certain indicators are selected and monitored during a specific period. During this period back-up plans are established which will be used as alternatives when losses need to be recovered;
- Transfer, when risks are transferred to an intermediary, usually a specialised institution; and
- Systematic reduction of risks, when all strategies and systems meant for reduction are systematically applied to reduce risks until an optimum level of risk has been attained.

(Toader *et al*., 2010:457)(Crain, 2014).

An effective Risk Management plan not only leads to reduced risks, but it can also enhance shareholder value and create a competitive advantage for an organisation which is able to manage its risks effectively. The section below discusses how value can be created or a competitive advantage can be obtained.

2.2.2 Competitive advantage through effective Risk Management

Organisations generally invest in Risk Management even though this comes at a price. When risk is reduced, it adds value to shareholders. The value added can be in the protection against costs, such as legal costs, re-financing costs, loss of key employees,

etc. Value is thus created if managers are able to decrease the organisation's exposure to specific risks in such a way that investors cannot diversify away (Godfrey, Merrill & Hansen, 2009:427). Amici, Fiordelisi, Masala, Ricci and Sist (2013:1393) is also of the opinion that value can by created through the opportunity that arises from exploiting risk reduction benefits that derive from a combination of activities that are not 100% correlated.

Given the value that effective Risk Management can create for stakeholders, it is important that Risk Management processes be disclosed in the annual Integrated Reports (IRs) of an organisation to ensure that shareholders are aware of value creation taking place through the disclosure of risks faced by the organisation and how these risks are being managed or mitigated. King IV provides recommendations on what needs to be disclosed in the IR of an organisation. This includes:

- Arrangements for managing risk and opportunity (IoD, 2016:37, 53);
- Key focus areas during the reporting period (IoD, 2016:37, 53);
- Mechanisms for monitoring and assessing adequacy and effectiveness of risk and opportunity management (IoD, 2016:37, 53); and
- How past performance, current operations and future strategic objectives are affected by uncertainties (IoD, 2016:37, 53)y.

The King IV Code also includes some of the requirements that have to be included in an organisation's IR, as specified in the IIRC's IR framework (IoD, 2016:37, 53).

A number of organisations have managed to go beyond compliance or cost-controlling risk defensive mechanisms and take more of an aggressive stance towards risk. They manage to leverage their Risk Management capabilities as a competitive advantage (Elahi, 2013:118). An example of such a competitive advantage being created, even as far back as 2000, was when the shared supplier for Nokia and Ericsson, Royal Phillip, was disrupted by a fire on 17 March 2000. Both cellphone companies were notified about the disruption at the same time. Ericsson took Royal Phillip on their word that operations

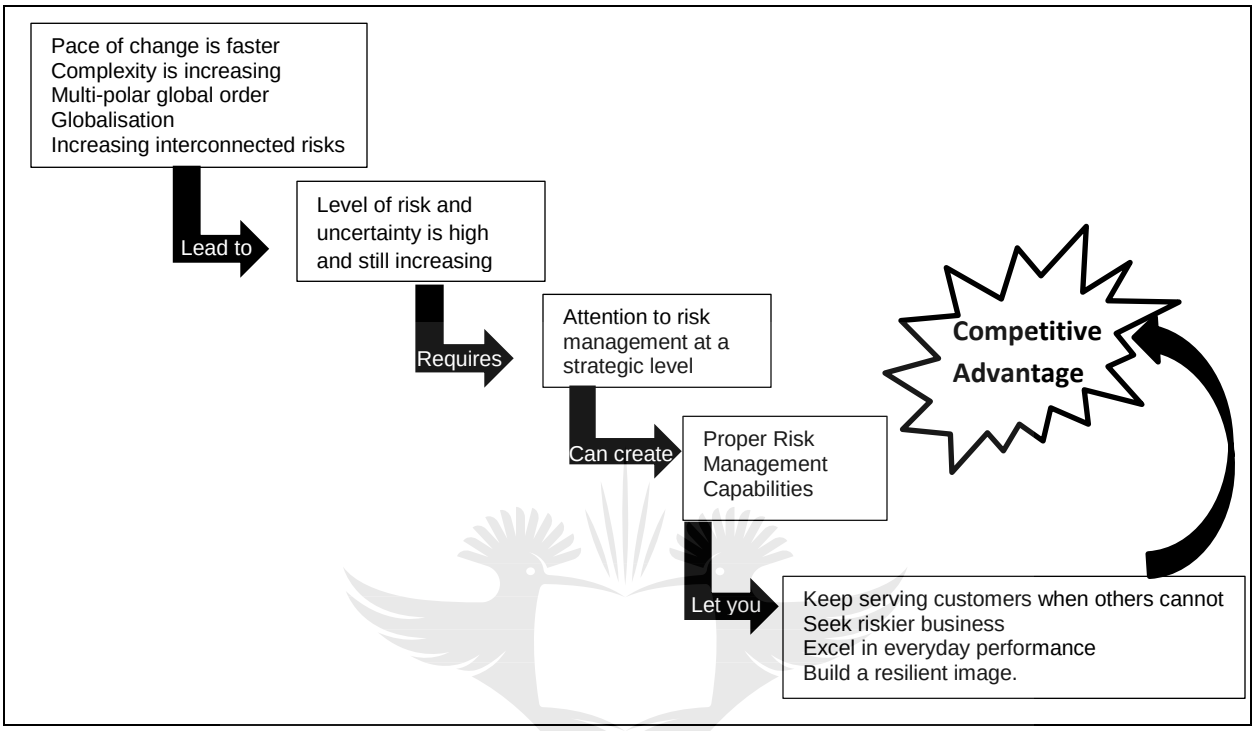
would resume within a week while Nokia took the disruption much more seriously. Nokia monitored the recovery process at Phillips very closely and soon realised the process would take longer than was initially said. Nokia therefore booked all available capacity at other suppliers and by the time Ericsson realised the magnitude of the situation, few suppliers were still available to produce components for Ericsson. In the second quarter of that year, Ericsson recorded a loss of $200 million in its cellphone division. The result of the above situation caused Nokia's market share to increase to 30% from 27% and Ericsson's market share to decrease to 9% from 12% (Elahi, 2013:119). Strenk further emphasises the importance of having an effective Risk Management process in place to gain a competitive advantage. He is of the opinion that in order to have a competitive advantage, one needs to be able to anticipate future potential risks. He provides a recent example in his study:

> "A manufacturing client used a variety of distribution channels to get their product into the marketplace. A detailed assessment of these key business partners revealed 'red flags' with one particular partner. The analysis resulted in a comprehensive plan of attack in anticipation of the event, which eventually came to fruition" (Strenk, 2013).

Another example of how competitive advantage was obtained through risk management is Sony. Sony faced a decrease in profitability in the television industry in the past few years. Through effective risk management, it became evident that a partnership was required in order to gain the relevant knowledge to improve the design of the televisions and lower the product range. Further research was also done to improve the sound and picture quality of the Bravia and LCD televisions. It also became evident that Sony had to expand into emerging markets in order to limit competition. Through proactive planning and effective research, Sony managed to turn around their profitability problems and became competitive again (Onick, 2014).

Figure 1 below illustrates how a competitive advantage can be obtained and maintained.

Figure 1: Gaining a competitive advantage through risk management



Source: (Elahi, 2013:128)

The next section examines how IT Risk Management differs from Risk Management in general.

2.3 IT RISK MANAGEMENT

2.3.1 Process of IT Risk Management

Jalba and Anicai (2012:0531) define IT risk as a sub-set of business risk, which is a consequence of business decisions. Over the past few decades, IT applications have become more susceptible to risk. This is due to the widespread use of computers, rapid development of the internet and the interconnectivity of computers. Another reason for the increased risk is users' improved IT skills. This increase in risk requires that greater attention be given to the management of IT Risk (Farah, 2011:13). IT Risk Management

is a sub-set of the overall Risk Management responsibilities of the BoD (Parent & Reich, 2009:137). The approach for IT Risk Management is, in general, the same as for Risk Management. The only difference between general Risk Management and IT Risk Management is the fact that IT Risk Management focuses first on IT risks and then those risks are incorporated into the general Risk Management of an organisation. The need to manage developing IT Risks leads to the development of several risk assessment frameworks by professional bodies (Al-Ahmad & Mohammad, 2013:29). The need to have a framework to assist in IT Risk Management can be attributed to the fact that research has shown that many boards pay insufficient attention to it. Studies have shown that the most common reason therefore is the fact that the IT Strategy does not align with the business strategies. Parent and Reich (2009:137) further indicate a significant lack of interest in IT by boards of directors.

One of the best adopted risk assessment frameworks for IT is the COBIT 4.1 (Control Objectives for Information and Related Technology). COBIT 4.1 was developed by the Information Systems Audit and Control Association (ISACA). COBIT adopts a more holistic approach to Risk Management than other standards. It focuses on identifying control objectives and the development of controls to meet the identified objectives. It consists of 34 processes that manage and control information and supporting technology. Research conducted on organisations over the years shows that COBIT has assisted in the alignment of business and IT to create an IT Governance Framework and establish IT Risk Management in organisations (Al-Ahmad *et al*., 2013:33). COBIT 5 aims to be the only framework for the governance and management of enterprise IT. It is primarily a guidance document that aims to provide guidance to organisations on how to manage IT risk / implement IT Governance (Harmer, 2012).

With IT becoming such a prominent factor in business, King IV has included a section under Risk Management that deals exclusively with IT Risk Management. Some of the recommendations made by King IV are discussed below.

2.3.2 Corporate Governance requirements for IT Governance

IT Governance can be defined as “the decision rights and accountability framework to encourage desirable behavior in using IT” (Juiz, Guerrero & Lera: 2014:14).The King IV report on Corporate Governance recognises the importance of IT in modern day organisations and the risks associated with IT. Therefore a separate section has been devoted specifically to governing IT risks. Thus, Principle 4.2 in King IV states that the “governing body should govern technology and information in a way that supports the organisation in defining its core purpose and achieving strategic objectives” (IoD, 2016:53).

Some of the recommendations made by King IV to assist companies in achieving the principle mentioned above state that the governing body should:

- Oversee that all IT related risks are properly managed (IoD, 2016:53);
- Provide the strategic direction to management in terms of IT (IoD, 2016:53);
- Approve a policy aimed at providing direction on how to use IT (IoD, 2016:53);
- Ensure the policy makes provision for the adoption of the relevant risk frameworks (IoD, 2016:53);
- Delegate the responsibility of implementing the policy to management (IoD, 2016:53);
- Oversee the effectiveness of technology use in the organisation (IoD, 2016:53);
- Periodically carry out a formal review of the adequacy and effectiveness of the organisation’s IT function (IoD, 2016:53).

King IV also provides guidance on IT Risk Management issues that have to be disclosed. The issues include:

- Structures and processes of IT Management (IoD, 2016:53);
- Key focus areas during the reporting period (IoD, 2016:53);

- Mechanisms in place for monitoring and assessing the adequacy and effectiveness of IT (IoD, 2016:53); and
- How past performance, current operations and future strategic objectives of the organisation are affected by digital development (IoD, 2016:53).

2.4 CONCLUSION

Chapter two focused on Risk Management, including IT Risk Management, and the importance thereof to an organisation. Risk Management is important to any organisation. When an organisation has an effective Risk Management process in place, it can create a competitive advantage as well as limiting risk to the organisation. An effective Risk Management process also enhances shareholder value. Shareholder value, however, can only be enhanced when the risks and controls are disclosed to stakeholders so that they have access to all information relating to the organisation when making decisions. Disclosure of the organisation's Risk Management process in the IR is not just of value to shareholders, but to all stakeholders, as well as being recommended practice in terms of King IV.

The traditional financial system was revolutionary when it was first implemented. Due to the increased complexities of legislation for accounting and corporate reporting, fully audited financial statements, although still critical, are insufficient to discharge the duty of accountability. The need has arisen to move from 'silo' reporting to Integrated Reporting which is more in line with an inclusive, sustainable capital market system (IoD, 2016:15).

Empirical study links

Disclosing of risks and how such risks are managed is important for all stakeholders to make informed investment decisions. A content analysis is conducted on whether organisations provide IRs, annual reports or Annual Integrated Reports. It will further determine whether IT risks have been disclosed in the IRs of the sample and whether corresponding Risk Management processes have been disclosed for the risks identified. The analysis of the reports is presented in Chapter Four of this study.

Chapter Three takes a closer look at the purpose of IRs and what the disclosure requirements are in terms of the IIRC's framework for IR.

CHAPTER 3
INTEGRATED REPORTING

3.1 INTRODUCTION

An IR aims to provide the potential investor or stakeholder with a well-rounded document containing all the relevant information needed to make informed decisions on the organisation. In 2010, as part of his Big Society Campaign, David Cameron said:

> "It's time we admitted that there's more to life than money and it's time we focused not just on GDP but on GWB – General well-being. Governments have failed to sufficiently internalize companies' environmental and social costs such that the consequent economic development is fully sustainable" (Eccles & Saltzman, 2011:61).

Abeysekera is of the opinion that in an era where news spreads as it happens through social media and internet, investors, society and governments are increasingly expecting companies to be held accountable for their actions to all stakeholders. The ultimate investor in an organisation, direct or indirect, is investing with a long-term view. This change in investor mindset has brought about a change in the investor landscape with investors being interested in not just financial information and returns, but also in the organisation's impact on the environment and society (Abeysekera, 2013:227).

These changes in stakeholder requirements are echoed by Reverte who believes that the increasingly complex business world and changes in stakeholder needs have resulted in a change in business and financial reporting over the years. This change in stakeholder needs requires organisations to disclose the risks they are facing as well as how these risks are being managed. Stakeholders are no longer interested in purely financial information but also want information on the organisation's environmental and social responsibilities as well as information on how these responsibilities fit in with the organisation's long or medium term goals and strategies (Reverte, 2015:285).

Reporting on social and environmental issues and responsibilities is not a new concept (Buhr, Beddington, O'Dwyer & Unerman, 2007:59). Reporting on social and environmental issues and responsibilities was initially incorporated into the annual financial reports of organisations (Buhr *et al*., 2007:58). This is emphasized by Hahn and Kühnen (2013:6) when saying that in the 1990's, the early stages of reporting on social and environmental issues, the reporting on social and environmental issues were done alongside the financial reports. The requirements of a variety of stakeholders on what elements need to be reported on increased over the past 20 years, causing the disclosure of these issues in separate, standalone, reports to the financial statements to become more complex and longer (de Villiers *et al*., 2014:1042). As a result, the need arose to combine the many reports into one report again (de Villiers *et al.*, 2014:1043). The new report would be different from prior reports as social, environmental, financial, Risk Management and governance information would be combined into the one report, which would be called an Integrated Report (de Villiers *et al.*, 2014:1043).

In its 2011 Discussion Paper, the International Integrated Reporting Council (IIRC) defines the Integrated Report as:

> '… a report to stakeholders on the strategy, performance and activities of the organisation in a manner that allows stakeholders to assess the ability of the organisation to create and sustain value over the short-, medium- and long-term. An effective Integrated Report reflects an appreciation that the organisation's ability to create and sustain value is based on financial, social, economic and environmental systems and by the quality of its relationships with its stakeholders' (IRC, 2011:6).

The next section examines the purpose of an IR.

3.2 PURPOSE OF INTEGRATED REPORTING

Loss of shareholder value due to corporate scandals, natural disasters and disregard for human rights has shown that non-financial information can have a devastating effect on

an organisation's bottom line (KPMG, 2011:1). This is echoed by the IIRC when it released its Discussion Paper in 2011 on the IR framework. It stated that corporate collapses over the past few years led many stakeholders to question the relevance and reliability of financial reports. Most reports provide information on the financial position of the organisation, but not enough on the social, environmental and economic challenges the organisation faces. Sustainability reports have similar weaknesses insofar as they can appear disconnected from the organisation's financial information (IRC, 2011:1).

The core concept of IRs revolves around the 'stakeholder inclusive' approach to provide a holistic and forward-looking picture of the organisation to all its stakeholders (KPMG, 2011:1). To provide such a picture, it is important to include the material risks an organisation faces as well as how these risks are being managed. It is equally important to ensure that the IT Risk Management is included if IT systems are deemed to be a material part of the organisation's operations. Integrated Reporting creates a common platform where governance, financial, social, intellectual and environmental capital can be brought together. It ensures the diverse dimensions of organisation's performance are unified under the organisation's vision and values and assists the organisation to demonstrate how its vision and values are internalised and externalised (Abeysekera 2013:232). When assessing the purpose of an IR, it can clearly be seen that it is in line with the purpose the IIRC had in mind in 2011, namely, "to report to stakeholders on the strategy, performance and activities of the organisation in a manner that enables stakeholders to assess the ability of the organisation to create and sustain value over the short, medium and long term" (IRC, 2011:6).

The following section discusses the development of the IR since the establishment of the International Integrated Reporting Committee (IIRC) in 2010.

3.3 DEVELOPMENT OF THE IR

Reporting on financial information became increasingly complex over the years, which lead to organisations reporting on social and environmental issues in separate reports,

some of which amounted to 200 pages (Cheng, Green, Conradie, Konishi & Romi, 2014:90). The early development of IRs can largely be linked to social and environmental reporting (de Villiers *et al*., 2014:1044). These disclosures were mostly related to managerial and organisational desires to meet what management perceived to be the requirements of stakeholders (Deegan, 2002:285). Different explanations have developed over the years as to why disclosures are made on social en environmental responsibilities. Some theories have developed over time, which include the stakeholder theory which state that organisations are responsible towards more stakeholders than just those who provide the capital. This theory suggests that management report on their social and environmental responsibilities to try and manipulate the most powerful stakeholders in the group (Mbekomize, 2013:68).

The first form of structure / framework / guidance to be given to IRs come from King III which was released in 2009 (Rensburg & Botha, 2014:146). King III requires organisations to release a report annually containing sufficient information on how the organisation affected the community's economic life in a positive and negative manner. It further requires disclosure on how the organisation performed during the year under review and what management's plans and expectations are for the year to come. Disclosure is often grouped under environmental, social and governance issues. It should also include how management intends to build on positive elements and limit negative elements (IOD, 2011: 12).

Integrated Reporting aims to create a more holistic way of thinking about the organisation (EY, 2012:11). This concept is taken further by Eccles and Churet who say that 'integrated thinking' requires finding a balance between managing short-term business imperatives and ongoing value creation. Sustainable value creation depends on an organisation's ability to remain competitive in an ever-changing environment (Churet & Eccles, 2014:56). In March 2010, the Johannesburg Stock Exchange (JSE) adopted King III and required all listed companies on the JSE to fully comply with King III as this was a listing requirement (Rensburg & Botha 2014: 146) and thus each listed company had to submit an IR. Van Zyl (2013) confirms the adoption by the JSE on 1 March 2010 to

comply with King III, requiring each listed company to submit an IR annually or explain why it has not met the requirements (van Zyl, 2013:906). The explanation from Professor Mervin King, who is the chairman and founder of the King Committee, on why IRs have been included as a disclosure requirement in King III can be found in the 2011 Discussion Paper released by the IIRC:

> "It is my belief that Integrated Reporting represents a significant and much-needed evolution of reporting practice and will start influencing behaviour. It is my hope that it will prompt a greater understanding of the sustainability challenges facing humankind" (IRC, 2011:2).

King IV, currently in draft format, requires an IR to 'tell the story' of how an organisation can create value in the future. This can be achieved by managing current risks that can have an impact on value creation in the future, especially if they are material risks. It requires an IR to adopt a forward-looking approach into the future and determine whether the organisation can deliver in terms of value (IoD, 2016:12). King IV is taking the release of an IR so seriously, that one of the principles of the report aims for "the governing body should ensure that reports and other disclosures enable stakeholders to make an informed assessment of the performance of the organisation and its ability to create value in a sustainable manner" (IoD, 2016:37). One of the recommended practices given by King IV stipulates that an organisation should issue an annual report in which all material information is presented in an integrated manner and provides a stakeholder with a clear, holistic, concise and understandable representation of the performance of the organisation. King IV requires some of the minimum requirements to be present in an IR as per the IIRC's IR Framework in its recommended practices (IoD, 2016:37).

Internationally, the first proper attempt to formalise IRs came about in 2010 when the International Integrated Reporting Committee, later the International Integrated Reporting Council (IIRC), was founded by two of the leading organisations in the field of accounting for sustainability, namely, The Prince's Accounting for Sustainability Project (A4S) and the Global Reporting Initiative (GRI) (Flower, 2015:1). The origins of these bodies can be traced back to a speech made by the Prince of Wales in 2009 when he called for the

existence of such a body (Flower, 2015:1). The primary purpose of the IIRC was to provide a concise (relatively few pages) report to indicate an organisation's most material social, environmental and economic actions, outcomes, risks (including IT Risks) and opportunities in such a manner that reflects the integrated nature of these factors for the organisation (de Villiers *et al*., 2014:1046). In order to provide a concise account indicating value creation over time, an organisation needs to communicate its strategy, governance, performance and prospects in the context of its external environment to show short-, medium- and long-term value creation (Cheng *et al.*, 2014:92).

In 2011, the IRC released a discussion paper outlining its objective in broad terms, which was to release one report, namely an IR, which aims to become an organisation's primary report (IRC, 2011:1). The IIRC identified four types of reports currently being issued by organisations, namely, Traditional Financial Statements, Management comments, Governance and Remuneration reports and Sustainability reports. Their goal is to ensure these four reports are better integrated with one another (Flower, 2015:3). In December 2013, the IIRC released a global framework to guide organisations in preparing IRs. The framework defines an IR as a "concise communication about how an organisation's strategy, governance, performance and prospects, in the context of its external environment lead to the creation of value over the short, medium and long term" (IIRC, 2013:7). In 2011, South Africa established its own IR commission, namely, the Integrated Reporting Committee of South Africa (IRCSA) which is chaired by Professor Mervin King (Cheng *et al*., 2014:93) (IRC, 2015:1). On 12 March 2014, the IRCSA endorsed the IIRC's framework for IR moving away from the stakeholder-inclusive IR framework used by South Africa to the framework for value creation for investors (de Villiers *et al.,* 2014:1050).

At present, South Africa is the only country where an IR is mandatory; other countries are still in the process of developing and publishing IRs (de Villiers *et al*., 2014:1050). Eccles and Saltzman confirm that other countries are preparing sustainability reports only on a voluntary basis where the stakeholder is provided with information on the organisation's environmental, social and governance performance (Eccles & Saltzman, 2011:58).

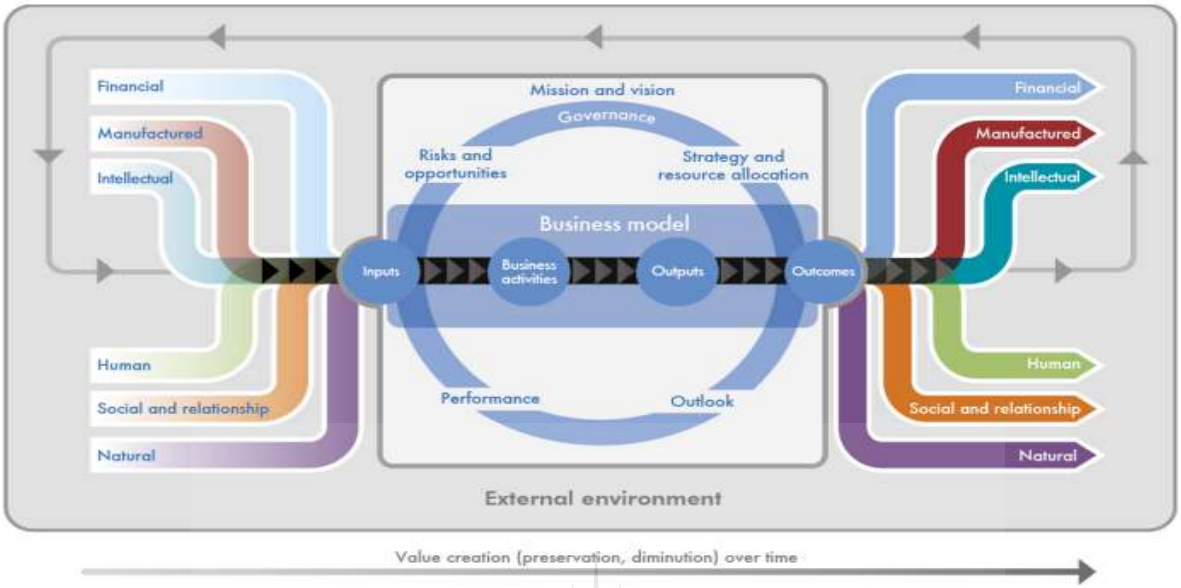
Preparing an IR for the first time forces an organisation to look at itself and its business models in a new way (IRC, 2011:1). A possible reason for organisations undergoing this process might be due to the possible benefits an organisation can obtain through the presentation of an IR. These benefits are included in the 2011 IR Discussion Paper (IRC, 2011:1).

The next section discusses the framework of IRs, as released by the IIRC, and specifically the sections relating to risk disclosure requirements.

3.4 IR FRAMEWORK

Essentially, the framework indicates that organisations use various types of resources to create value. These resources are commonly referred to as capitals and the IIRC has identified six capitals used to create value, namely, Manufactured, Intellectual, Human, Social and Relationship, Natural and Financial (Cheng *et al*. 2014:95) (IIRC, 2013:11). The objective of an IR is to improve the accountability and stewardship of the six broad base capitals of an organisation and their interdependencies (Busco, Frigo, Quattrone & Riccaboni, 2013:35). Figure 2 on the following page illustrates how these capitals work together to create value for an organisation.

Figure 2: Value creation through the six capitals resources



Source: IIRC, 2013:13

The international IR framework was released by the IIRC in December 2013. The purpose of the framework is to assist organisations in establishing concepts, guiding principles and content elements that govern the overall content of the report (Busco *et al*., 2013:35). The intervention of the framework is to provide a balance between flexibility and prescription. The framework is therefore not rule-based, but rather principle-based (IIRC, 2013:4). Furthermore, the framework does not specify whether the IR must be a separate report or whether it can be combined with other reports as long as it is clearly distinguishable (IIRC, 2013:4). Although the framework is not prescriptive in the key and material performance indicators to be included, it does have a small amount of requirements that have to be met before an IR can be released (IIRC, 2013:5).

Since the purpose of this study is focused on the disclosure of IT Risk Management in IR reports, the emphasis is placed solely on the guiding principle of Materiality and two of the other elements in the framework, namely, Risks and Opportunities and Outlook. The IR framework (2013) discusses each element as follows:

Materiality

"An IR should disclose information about matters that substantively affect the organisation's ability to create value over the short, medium and long term."

The process followed to identify such matters requires of management to identify any relevant matters that will affect the organisation's ability to create value, determine the importance of identified matters or the significance of their impact, and lastly, to prioritise them. This process needs to be followed for all positive and negative matters, including risks and opportunities, favourable and unfavourable or performance prospects. When determining whether something is material, consideration should be given to quantitative and qualitative facts, financial, operational, strategic, reputational and regulatory perspectives and whether the internal or external area is affected (IIRC, 2013:18).

Risks and Opportunities

The framework requires an IR to answer the following question: "What are the specific risks and opportunities that affect the organisation's ability to create value over the short, medium and long term and how is the organisation dealing with them?"

In an IR the key risks and opportunities that are specific to the organisation need to be included, specifically those that affect the organisation's continued availability, quality and affordability of relevant capitals over the short, medium and long term.

The risks identified can be internal, external or a combination of the two and can include some of the following: change in the business environment, speed and effect of technological change and change in the legislative and regulatory environment (IIRC, 2013:27).

Outlook

The framework requires an IR to answer the following question: "What challenges and uncertainties is the organisation likely to encounter in pursuing its strategy, and what are the potential implications for its business model and future performance?"

An IR ordinarily provides information on anticipated changes over time and indicates the organisation's expectations of the external environment in the short, medium and long term. It helps to determine how the organisation will be affected and is currently equipped to deal with critical challenges and uncertainties that are likely to arise (IIRC, 2013:28).

Source: IIRC, 2013

3.5 CONCLUSION

It is therefore evident that an IR is a suitable report that an organisation should compile to provide its stakeholders with enough information to make informed decisions. Although the IR needs to include all material information, as identified by the organisation's management, the IIRC still requires reports to be as concise as possible (IRC, 2011:1) and must be written in a clear and understandable language (IRC, 2011:1). Leigh Roberts, co-founder of the Integrated Reporting Committee (IRC) of South Africa and member of the Integrated Thinking Task Force of the South African Institute of Chartered Accountants (SAICA), agrees that the best reports on the JSE consist of 100 pages or less. Sometimes an IR can contain as many as 300 pages, which poses the risk of vital information being buried among other, less important information (Roberts, 2015). EY (2012:5) further emphasise the importance of the length of an IR, indicating that the most successful IRs are the simplest ones. Although the IIRC requires a concise report, it allows for information in the report to be linked to more detailed information, electronically or on paper, allowing stakeholders to obtain a more detailed account according to their specific needs (IIRC, 2013:8). De Villiers *et al*. confirms that the report should be electronic to allow users to drill down to elements and other information they are interested in (de Villiers *et al.,* 2014:1046).

Empirical study links

Having a report in which stakeholders can see how the firm creates value is an important requirement of the modern stakeholder. The modern day stakeholder prefers an IR containing disclosures of all material information, as determined by management, that can have an impact on the organisation's ability to create value. The content analysis in this study determines how material risks have been identified and whether they have been disclosed. It also determines whether IT Risk has been included and whether the elements of the IR, especially those relating to IT Risk and IT Risk Management, are clearly identifiable and understandable to the stakeholder.

The following chapter discusses the empirical study conducted on a selection of IRs to determine whether they are in compliance with the IIRC framework, specifically in terms of the disclosure of IT Risk Management.

CHAPTER 4
EMPIRICAL STUDY

4.1 INTRODUCTION

As stated in Chapter One, the objective of this study is to determine to what extent IT Risk and IT Risk Management are disclosed in the IRs of organisations. The methodology followed to achieve this objective is a literature review, based on which a critical analysis was conducted to identify IT risks that organisations are exposed to as well as how they are being managed. It also provided guidance on how the IR should look, what should be considered when preparing an IR and what should be included. The results of the literature review (Chapters Two to Four) form the basis for a content analysis of the IRs of the Top 40 listed companies on the Johannesburg Stock Exchange (JSE).

4.2 APPROACH TO THE EMPIRICAL STUDY

4.2.1 Selection of the population

The population selected for testing consisted of the Top 40 listed companies on the JSE. The JSE Top 40 companies are reviewed on a quarterly basis in March, June, September and December every year as part of the FTSE / JSE quarterly index review (2016(a):22). The population for the empirical study was selected based on the Index as at 7 September 2016 (JSE, 2016(b)). The reason for selecting the Top 40 companies of the JSE as a population is due to the fact that they represent 83.31% market share of the total market on 7 September 2016 (JSE, 2016(b)). An expectation is created that if the Top 40 listed companies on the JSE are providing quality IRs, smaller companies will have a good example to work from when producing their own IRs. All Top 40 listed companies were included in the empirical study (refer to Annexure B for a detailed list of the companies).

4.2.2 Methods applied in the empirical study

The empirical study consists of a content analysis of the IRs or Annual IRs of the Top 40 listed companies on the JSE. A content analysis have been selected as the research method as data can be obtained from independent sources ensuring better comparability to each other as there is one standard that has to be met. Since all IR reports are on the companies websites, it is available to use and more easily obtainable. No contact were made with any of the companies selected, leading to the study performed being a desk top study. There are limitations to this study as the empirical study is limited to the Top 40 listed companies of the JSE only, and may not be representative of the smaller listed entities on the JSE. Content analysis is, however, widely recognised and supported as a suitable research instrument for understanding and analysing the characteristics of a selected population (Marx & Mohammadali-Haji, 2014:235). This is confirmed by Ceci and Iubatti who agree that content analysis can be used to analyse a given set of data to ensure the objective, systematic and quantitative description of the communication contents of the data set (Ceci & Iubatti, 2012:566). Content analysis allows the user to test the theoretical issues by enhancing the understanding of the data (Elo & Kyngäs, 2008:108).

4.2.3 Investigation of IRs

The most recent IRs of the Top 40 companies on the JSE were obtained from each organisation's website and investigated between 10 September 2016 and 19 September 2016. The elements, disclosure of Risk Management, analysed in the IR were based on the information obtained from the literature review. The research method used to obtain the information was a qualitative research method. The analysis was performed using a checklist against which the IRs of the companies were measured. The checklist was developed using information obtained from the literature review with the results tabled under Interpretation of Analysis Findings.

4.3 RESEARCH CONTROL

The research control to this analysis was the fact that 100% of the IRs of all the Top 40 listed companies were analysed.

4.4 INTERPRETATION OF ANALYSIS FINDINGS

4.4.1 Type of report released annually

i. Objective of the analysis

The purpose of this section is to determine how many of the Top 40 listed companies on the JSE produce an IR and in what format.

ii. Findings and deductions

Table 1: Type of reporting

Type	Number	%
Integrated Annual Report (annual report and financial statements combined)	26	65%
Separate Annual Report and Integrated Report	12	30%
Annual Report only (no Integrated Report)	2	5%
Total	**40**	**100%**

Source: Own analysis

The above findings indicate that most of the companies provide annual IRs consisting of Annual Financial Statements and IR information, as required by the IR Framework. The layout of these reports takes the form of the annual report of a company where the elements of an IR have been included to create one, complex report. The annual IR, where the elements of the IR have been included in the annual reports, clearly indicates

the relevant information as required by the IR framework and the financial statement section of the report is clearly indicated. However, some companies merely renamed their annual reports as Integrated Annual Reports in order to give the impression that an IR was provided, when that was not the case.

It became evident that the format of the reports, irrespective of whether they were annual reports or integrated annual reports, was fairly similar. Both of these reports generally contain the following sections: strategic overview of the organisation, business review, governance report, key risks and opportunities or risk management report or material risk, financial overview or financial statements.

The companies which produced standalone IRs provided a relatively concise document which included the information required by the IR framework. Risks were clearly indicated and there was sufficient reference made to other reports available on the organisation's website where more details could be obtained.

4.4.2 Disclosure of how material risks are determined

i. Objective of the analysis

The objective of this part of the analysis was to determine which of the 38 companies that produced IRs or Annual Integrated Reports provided stakeholders with an explanation as to how the material issues / risks were identified.

ii. Findings and deductions

Table 2: Disclosure of whether discussion is provided on how material risks have been identified

Element	Numbers		Percentages		**Total**
	Yes	No	Yes	No	
Discussion provided on how material risks have been identified	23	15	61%	39%	**38**

Source: Own analysis

The analysis indicated that only 23 of the companies provided information to stakeholders on how material risks were being identified. The companies that did not provide explanations on how material risks were identified, simply provided the disclosure of their material risks. Some of the main processes followed by the companies to identify material risks included, but were not limited to, the following considerations:

- Determining the likelihood and potential impact of the risk on the organisation;
- Identifying the risks that could lead to a breach in the organisation's risk appetite and impact the value chain negatively;
- Issues that could have an impact on achieving the commercial viability and social vision in the medium term;
- Risks that could have a material impact on the reputation of the organisation;
- Key matters that could have an impact on the organisation achieving its strategic objectives and creating value; and
- Matters that could affect the business model, future performance, solvency or liquidity of the organisation.

4.4.3 Disclosure of material risks

i. Objective of the analysis

The objective of this part of the analysis was to determine that of the 38 companies which provided an IR or Annual Integrated Report, how many disclosed material risks that could have an impact on value creation over the short, medium and long term. Furthermore, this part also sought to determine how many of the companies which did disclose material risks, included IT risk as a material risk. Where IT risks have been included as a material risk, the analysis went further to determine whether the IT risk was easily identifiable or not.

ii. Findings and deductions

Table 3: Disclosure of material risk

Element	Numbers		Percentages		**Total**
	Yes	No	Yes	No	
Material risk is properly disclosed	35	3	92%	8%	**38**
IT Risk is included in Material risk	23	12	66%	34%	**35**
IT Risk is easily identifiable	20	3	87%	13%	**23**

Source: Own analyses

The findings above indicated that the majority of the organisations (92%) provided disclosure of their material risks. These risks were spread throughout the organisation and were not limited to only financial risks. It is interesting to note that IT is deemed a significant risk for only 66% of the population. Of the 23 companies which included IT risk as part of material risks, 20 disclosed the IT risks in a manner that was easily identifiable to the stakeholder. Whether IT risk was deemed a material risk depended on the industry type. Throughout the banking industry, IT was deemed to be a material risk.

Most of the mining organisations did not deem IT risk as a material risk, however, they all disclosed that IT Governance was being applied appropriately. Those organisations in the mining industry which identified IT risk as a material risk did so primarily in terms of the risk of unauthorised access to their systems, confidential information and security breaches that could take place. Risks that were material to the mining industry included the economy, constant supply of electricity and climate change. The retail industry, in general, did not classify IT risk as a material risk with the exception of the Woolworths group where IT risk was disclosed as being a material risk. Other industries where IT risk was classified as a material risk included the beer industry, the printing industry, telecommunications, the medical industry, packaging, investment (primarily due to client information that has to be kept confidential) and the medical aid industry.

The results of the analysis further indicated that where material risks were discussed, including IT risks, the risks were easily identifiable.

4.4.4 The detail in which IT risk is disclosed

i. Objective of the analysis

This part of the analysis sought to determine the level of detail in which the IT risks were disclosed, in particular, to establish whether there was simply a high level mention of IT risks or whether risks were discussed individually.

ii. Findings and deductions

Table 4: Detail in which IT risks are disclosed

Element	Numbers		Percentages		**Total**
	Yes	No	Yes	No	
IT Risk disclosed with sufficient detail	20	3	87%	13%	**23**

Source: Own analysis

From Table 4 on the previous page, it is evident that 87% of the companies disclosed their IT risks with enough detail to give the stakeholder sufficient information on their IT risks. Some of the material IT risks that were identified and disclosed during the analysis included, but were not limited to:

- Cyber attacks which are growing more sophisticated on a daily basis and can have an adverse impact on the marketing of an organisation as well as increased money laundering and financial fraud;
- Disruption to IT systems which could consequently lead to the loss of valuable information;
- Unauthorised access, through breaches in the IT system, to confidential information and possible contraventions of the POPI Act;
- IT malfunction that could lead to loss of data and key information;
- The risk that, due to the fast changing IT environment, a competitive advantage may not be maintained;
- Infrastructure might not be able to keep up with changes in the IT environment;
- The organisation may have inadequate systems / investments in IT;
- The IT system may not be fully aligned to support business processes and procedures; and
- Disruption in business operations and business continuity.

Risks differ from organisation to organisation, but the one threat that is consistent in each organisation is the risk that access may be obtained by unauthorised persons to sensitive information.

4.4.5 Extent of detail in which IT Risk Management is disclosed

i. Objective of analysis

The purpose of this part of the analysis was to determine how many of the companies that disclosed IT risk with sufficient detail, disclosed the procedures followed to manage this risk with an equal amount of attention to detail.

ii. Findings and deductions

Table 5: Detailed IT Risk Management disclosure

Element	Numbers		Percentages		**Total**
	Yes	No	Yes	No	
Detail with which IT Risk Management is disclosed	20	3	87%	13%	**23**

Source: Own analysis

Based on the analysis, it was evident that all organisations provided a general Risk Management process that was followed by them to manage risks. Organisations which disclosed IT risk as part of their material risks provided detailed Risk Management procedures as well. This meant that the Risk Management processes were either included next to the risk in the disclosure of the material risks, or they were provided in the Risk Management report included in the Integrated Annual Reports. Disclosure of IT Risk Management procedures could not be traced to specific types of Risk Management reports provided by the organisations. Where separate Risk Management reports were produced, organisations appeared to base these on disclosure in terms of IT Governance, as required by King III and King IV. Where IT risks were included in the material disclosure, detailed Risk Management processes were disclosed. Some of the common IT Risk Management procedures followed by the companies included, but were not limited to:

- Implementing Risk Management procedures according to the framework provided by Committee for Sponsoring Organisations (COSO);
- Constant development and implementation of IT security policies;
- Increased investment to improve IT security awareness;
- Intelligence and implementation of sound security processes;
- Building necessary resilience into systems to manage and identify cybercrime;
- Continuously assessing threats and adapting controls for risk;
- Implementing logical access controls comprehensively'
- Increasing customers' and clients' awareness of cyber threats and how to prevent these;
- Implementing and maintaining antivirus software;
- Putting into place policies and monitoring these to ensure business continuity;
- Taking out cyber insurance to assist with major cyber breaches; and
- Performing regular tests to determine the ability of the organisation to recover data in the prescribed timeframe.

4.5 SUMMATIVE OBSERVATIONS

From the analysis conducted above, the results indicate that most companies disclose material risk separately and for 66% of those companies, IT risks are considered to be a material risk. Of the 66% which consider IT risk a material risk, IT risk can clearly be identified in 87% of those reports. Of the 66% companies where IT risk was included in their IR as part of their material risks, 87% provided details on the specific risks faced as well as how the respective risks were managed.

4.6 CONCLUSION

In this chapter, the methodology adopted for the empirical study was discussed and the results of the study were analysed. The findings indicate that almost all of the Top 40 listed companies on the JSE presented IR reports, although not all of the companies

presented the reports as a separate report from the Annual Financial Statements. The findings also showed that all the companies indicated what their major risks were and for most of the companies, IT risks were included as part of material risks. The management of these IT risks was outlined in sufficient detail revealing information on how each risk was being managed by the organisation. The findings further indicate that the management of these organisations is committed to improving the security and reliability of their IT systems and to minimise the risks associated with those IT risks.

In Chapter Five the conclusion of the literature study and the empirical study is presented and recommendations are made for future research opportunities.

CHAPTER 5
CONCLUSION

5.1 INTRODUCTION

In this chapter the significant findings that emerged from the literature in Chapters Two and Three as well as the significant findings from the empirical study in Chapter Four are summarised. Areas for future research are also highlighted.

5.2 DEDUCTIONS AND RECOMMENDATIONS

5.2.1 Literature review

The literature reviewed indicated that most organisations in the 21st century are dependent on some form of IT system. The presence of these systems and reliance on these systems has created significantly increased levels of risk than in the past. In order to ensure the sustainability of the organisation, management has to ensure all risks, including IT Risks, are properly managed.

Some of the main findings from the literature review include:

As per the objectives set out in Chapter one of this study the findings that is evident from the respective chapters are as follows:

Chapter two where the aim was to determine IT Risk Management and the Governance thereof in terms of King.

- Most modern organisations rely in IT systems to do business;
- IT has brought with it an increasing number of risks over the past few years. Some of these risks include unauthorised access to systems, unauthorised changes to confidential data and loss of information;

- Management needs to ensure that proper procedures are in place to manage such risks and reduce them to an acceptable level. Risks which are managed effectively can possibly lead to a competitive advantage for the organisation;

Findings from Chapter three, with the objective to determine what the purpose of an IR is and how IT Risks and the management thereof should be disclosed in the IR are:

- The purpose of IRs is to provide stakeholders with a well-rounded set of information on an organisation to enable them to make informed decisions. The IIRC intended for the IR to be a short and concise document; and
- Although there is no specific mention of IT Risk Management disclosure in the IR Framework, the framework requires that all material issues, including risks and opportunities that might have an impact on the organisation's ability to create value over the short, medium and long term, be properly disclosed, as well as the organisation's management of such issues.

5.2.2 Empirical study

Based on the information drawn from the literature review and the results of the empirical study, the following conclusions can be drawn:

- Most organisations find it very difficult to provide a separate IR and have included IR elements in their Annual Reports. These reports are called Annual Integrated Reports;
- Material IT risks faced by organisations are disclosed by most of the Top 40 listed companies, but all not all of these companies classify IT risk as part of their material risks;
- Relevant IT Risk Management Processes implemented in terms of King III have been disclosed by the companies, however, specific IT Risk Management procedures in terms of each specific risk have not always been discussed clearly; and

- The IR Framework requires that the risks indicate how they will affect the companies in creating value over the short, medium and long term. This was not disclosed in any of the reports.

5.2.3 Recommendations

Based on the above findings, the following recommendations can be made:

- Management and those responsible for the preparation of financial information need to obtain a thorough understanding of the purpose of an IR and the goals it should achieve with regard to stakeholders;
- Those charged with governance and those responsible for the preparation of financial information need to ensure that they have a thorough understanding of the IR framework as this is a useful document which provides guidance on preparing an IR; and
- When assessing risks, it is important for modern day organisations to not just focus on financial risks or traditional risks that they currently face or may have faced over the years. Careful consideration should also be given to IT risks faced by organisations and to assess their potential impact in the future. Organisations must also include in their assessment the procedures to be implemented to manage the identified risks. It is crucial for IT risk to be included in risk assessments because IT has become the focal point of most modern day organisations.

5.3 AREAS FOR FUTURE RESEARCH

The following areas have been identified for future research:

- An investigation into the difficulties organisations experience, preventing them from disclosing risks in the short, medium and long term in an IR;

- The extent of competitive advantage to be gained through effective IT Risk Management procedures; and
- The impact of King IV on IT Governance in terms of current IT Governance according to King III and any related disclosure.

5.4 CONCLUSION

This study investigated the extent to which IT Risk Management is disclosed in the IRs of the Top 40 listed companies on the JSE. It was found that most companies have included IT risk as part of material risks faced. However, although these companies did include Risk Management in their disclosures, not all of them provided sufficient evidence of detailed Risk Management procedures to be followed for each identified risk. Some provided a blanket Risk Management process discussion.

The empirical study showed that most companies indicated IT risk as a critical risk, especially in terms of risks relating to continuity in the event of a disaster and protection of personal / confidential information. It became clear during the course of this study that there are still improvements to be made in terms of Risk Management disclosure and the grouping of risks in the short, medium and long term when disclosure of the above is made in the IR.

To ensure greater transparency and added value for stakeholders, it is essential that management of companies or the preparers of financial information have a thorough understanding of IRs and their purpose as well as the disclosure requirements that need to be met, especially in terms of the level of detail in which certain elements have to be disclosed.

BIBLIOGRAPHY

Abeysekera, I. (2013). A template for integrated reporting. *Journal of Intellectual Capital,* 14(2):227-245.

Adeusi, S. O., Akeke, N. I., Adebisi, O. S., Oladunjoye, O. (2014). Risk management and financial performance of banks in Nigeria. *European Journal of Business and Management,* 6(13):336-342.

Ahmed, F., Capretz, L.F., Sandhu, M.A. & Raza, A. (2014). Analysis of risks faced by information technology offshore outsourcing service providers. *IET Software,* 8(6):279-284.

Al-Ahmad, W. & Mohammad, B. (2013). Addressing information security risks by adopting standards. *International Journal of Information Security Science,* 2(2):28-43.

Amici, A., Fiordelisi, F., Masala, D., Ricci, O., Sist, F. (2013). Value creation in banking through strategic alliances and joint ventures. *Journal of Banking & Finance, 37(5):1386-1396.*

Amran, A., Manaf Rosli Bin, A. & Che Haat, M.H., (2008). Risk reporting: An exploratory study on risk management disclosure in Malaysian annual reports. *Managerial Auditing Journal,* 24(1):39-57.

Atyam, S.B. (2010). Effectiveness of security control risk assessments for enterprises: Assessment of the business perspective of security risks. *Information Security Journal: A Global Perspective,* 19(6):343-350.

Bannerman, P.L. (2008). Risk and risk management in software projects: A reassessment. *Journal of Systems and Software,* 81(12):2118-2133.

Buhr, N., Unerman, J., Bebbington, J. & O'Dwyer, B. (2007). Histories of and rationales for sustainability reporting. *Sustainability Accounting and Accountability,* 57-69.

Busco, C., Frigo, M.L., Quattrone, P. & Riccaboni, A. (2013). Redefining corporate accountability through integrated reporting: What happens when values and value creation meet? *Strategic Finance,* 95(2):33-42.

Ceci, F. & Iubatti, D. (2012). Personal relationships and innovation diffusion in SME networks: A content analysis approach. *Research Policy,* 41(3):565-579.

Cheng, M., Green, W., Conradie, P., Konishi, N. & Romi, A. (2014). The international integrated reporting framework: Key issues and future research opportunities. *Journal of International Financial Management & Accounting,* 25(1):90-119.

Churet, C. & Eccles, R.G. (2014). Integrated reporting, quality of management and financial performance. *Journal of Applied Corporate Finance,* 26(1):56-64.

Crain, J. (2014). 4 Key steps to a risk management plan. Available from: http://gibraltarrisk.com/content/4-key-steps-risk-management-plan. (Accessed 27 March 2017).

Croson, P. L., Drevich, D. C. (2013). Information technology and business-level strategy: Toward an integrated theoretical perspective. *MIS Quarterly,* 37(2):483-509.

de Villiers, C., Rinaldi, L & Unerman, J. (2014). Integrated reporting: Insights, gaps and an agenda for future research. *Accounting, Auditing & Accountability Journal,* 27(7):1042-1067.

Deegan, C. (2002). Introduction: The legitimising effect of social and environmental disclosures: A theoretical foundation. *Accounting, Auditing & Accountability Journal,* 15(3):282-311.

Deumes, R. (2008). Corporate risk reporting: A content analysis of narrative risk disclosures in prospectuses. *Journal of Business Communication,* 45(2):120-157.

Eccles, R.G. & Saltzman, D. (2011). Achieving sustainability through integrated reporting. *Stanford social innovation review summer,* 59:59-61.

Ecker-Lala, W. (2010). Risk management for enterprises. *Hyperion International Journal of Econophysics & New Economy,* 3(2):217-223.

Elahi, E. (2013). Risk management: The next source of competitive advantage. *Foresight,* 15(2):117-131.

Elo, S. & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing,* 62(1):107-115.

EY (2006). *IT Governance: Improving IT performance, delivering business value.* Available from: www.ncc.co.uk/download.php. (Accessed on 6 June 2016).

EY (2012). Integrated Reporting: General impressions. Available from: http://www.ey.com/Publication/vwLUAssets/EY-excellence-in-integrated-reporting-awards-2012/$FILE/EY-excellence-in-integrated-reporting-awards-2012.pdf. (Accessed on 5 September 2016).

Farah, B. (2011). A maturity model for the management of information technology risk. *International Journal of Technology, Knowledge & Society,* 7(1):13-25.

Flower, J. (2015). The international integrated reporting council: A story of failure. *Critical Perspectives on Accounting,* 27:1-17.

Gao, P. (2010). Disclosure quality, cost of capital and investor welfare. *The Accounting Review,* 85(1):1-29.

Gartenberg, M. (2006). Technology now defines the business. *Computerworld*, 40(31):18-19.

Godfrey, P.C., Merrill, C.B. & Hansen, J.M. (2009). The relationship between corporate social responsibility and shareholder value: An empirical test of the risk management hypothesis. *Strategic Management Journal,* 30(4):425-445.

Hahn, E., Kühnen, M., (2013). Determinants of sustainability reporting: a review of results, trends, theory, and opportunities in an expanding field of research. *Journal of cleaner production, 29:5-21.*

Harmer, J. (2012). Cobit 5 All together now. Available from: http://www.bcs.org/upload/pdf/smsg-210612.pdf. (Accessed on 27 March 2017).

Hayes, F. (2003). Business leads IT. *Computerworld,* 37(18):54.

International Integrated Reporting Committee (IIRC) (2013). *The International <IR> Framework.* Available from: https://integratedreporting.org/wp-content/uploads/2013/12/13-12-08-THE-INTERNATIONAL-IR-FRAMEWORK-2-1.pdf (Accessed on 28 August 2016).

Integrated Reporting Committee (IRC) (2011). *Framework for Integrated Reporting and the Integrated Report - Discussion Paper.* Available from: http://www.sustainabilitysa.org/Portals/0/IRC%20of%20SA%20Integrated%20Reporting%20Guide%20Jan%2011.pdf (Accessed on 28 August 2016).

Integrated Reporting Committee (IRC) (2015). *Reporting on outcomes, an information paper.* Available from: http://www.integratedreportingsa.org/Portals/0/Documents/IRCReportingOutcomesIP.pdf (Accessed on 28 August 2016).

International Accounting Standard Board (IASB) (2011). *IFRS Textbook*. London: IFRS Foundation.

Institute of Directors (IoD) (2011). *SAICA Legislation Textbook 2011/2012*. Durban: Lexis Nexis.

Institute of Directors (IoD) (2016). *King Code IV on Corporate Governance in South Africa.* Available from: http://bit.ly/KingIVdraft. (Accessed on 10 September 2016).

Jalba, L. & Anicai, O. (2012). Innovation in managing the IT risks of entrepreneurship risk management. *Annals of DAAM and Conference Proceedings*, 23(1):0529-0532.

Johannesburg Stock Exchange Limited (JSE) (2016(a)). *Ground Rules for FTSE / JSE Africa Index Series.* Available from: https://www.jse.co.za/contenct/JSEIndex ClassificationandCodesItems/FTSE%20JSE%20Ground%20Rules.pdf. (Accessed on 17 September 2016).

Johannesburg Stock Exchange Limited (JSE(b)) (info@jse.co.za). 7 September 2016. *RE: Indices - Top 40 listed companies.* Email to Hols-du Preez, C. (chohls@uj.ac.za).

Juiz, C., Guerrero, C. & Lera, I. (2014). Implementing good governance principles for the public sector in information technology governance frameworks. *Open Journal of Accounting*, (3):9-27.

Ko, M. & Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology Management,* 17(2):13-22.

KPMG (2011). Integrated reporting: Understanding the requirements. Available from: https://www.kpmg.com/ZA/en/IssuesAndInsights/ArticlesPublications/General-Industries-Publications/Documents/Integrated%20reporting%20-%20Understanding%20the%20requirements.pdf. (Accessed on 16 September 2016).

Maillart, T. & Sornette, D. (2010). Heavy-tailed distribution of cyber risks. *The European Physical Journal B,* 75(3):357-364.

Marx, B. (2008). *An analysis of the development, status and functioning of audit committees at large listed companies in South Africa.* PhD thesis. Johannesburg: University of Johannesburg.

Marx, B. & Mohammadali-Haji, A. (2014). Emerging trends in accounting: An analysis of integrated reporting practices by South African top 40 listed companies. *Journal of Economic and Financial Sciences,* 7(1):233-252.

Mbekomize, C. J. (2013). Social and environmental disclosure by parastatals and companies listed on the Botswana Stock Exchange. *Journal of Management and Sustainability,* 3(3):66-75

McKinsey & Company. (2016). The CEO guide to boards. Available from: http://www.mckinsey.com/global-themes/leadership/the-ceo-guide-to-boards. (Accessed on 27 March 2017).

Mercury Business Technology Optimization (2005). *IT governance challenges and best practices*. Available from: http://www.iworksmarcom.com/MercuryWhitepaper.pdf. (Accessed on 5 June 2016).

Miihkinen, A. (2012). What drives quality of firm risk disclosure?: The impact of a national disclosure standard and reporting incentives under IFRS. *The International Journal of Accounting,* 47(4):437-468.

Nel, I. (2010) *An investigation into business continuity risks and related business continuity plan.* Master's thesis. Johannesburg: University of Johannesburg.

Nikolić, B. & Ružić-Dimitrijević, L. (2009). Risk assessment of information technology systems. *Issues in Informing Science and Information Technology,* 6:595-615.

Nocco, B.W. & Stulz, R.M. (2006). Enterprise risk management: Theory and practice. *Journal of Applied Corporate Finance,* 18(4):8-20.

Nolan, R. & McFarlan, F.W. (2005). Information technology and the board of directors. *Harvard Business Review,* 83(10):96.

Onick, A. (2014). *Competitive Advantage of SONY Corporation*. Available from: http://sonycorporation1.blogspot.co.za/. (Accessed on 29 September 2016).

Oxford Dictionary (2016). *Definition of Spam.* Available from: https://en.oxforddictionaries.com/definition/spam. (Accessed on 1 August 2016).

Parent, M. & Reich, B.H. (2009). Governing information technology risk. *California Management Review,* 51(3):134-152.

Pekker, M. (2010). *20 common types of computer viruses and other malicious programs*. Available from: http://files-recovery.blogspot.co.za. (Accessed on 1 August 2016).

PricewaterhouseCoopers (PwC) (2009). *Executive guide to King III*: *King's Counsel – Understanding and unlocking the benefits of sound corporate governance.* Johannesburg: PricewaterhouseCoopers.

PricewaterhouseCoopers (PwC) (2006). *IT Governance in Practice: Insight from Leading CIOs.* Johannesburg: PricewaterhouseCoopers.

Rennekamp, K. (2012). Processing fluency and investors' reactions to disclosure readability. *Journal of Accounting Research,* 50(5):1319-1354.

Rensburg, R. & Botha, E. (2014). Is integrated reporting the silver bullet of financial communication? A stakeholder perspective from South Africa. *Public Relations Review,* 40(2):144-152.

Reverte, C. (2015). The integrated reporting movement: Meaning, momentum, motives and materiality. *Journal of Cleaner Production,* 86:285-288.

Rivard, S., Raymond, L. & Verreault, D. (2006). Resource-based view and competitive strategy: An integrated model of the contribution of information technology to firm performance. *The Journal of Strategic Information Systems,* 15(1):29-50.

Roberts, L. (2015). *Special Feature: Integrated Reporting.* Available from: http://www.accountancysa.org.za/special-feature-integrated-reporting/. (Accessed on 5 September 2016).

Sarrazin, H. & Willmott, P. (2016). Adapting your board to the digital age. Available from: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/adapting-your-board-to-the-digital-age. (Accessed on 27 March 2017).

South African Institute of Chartered Accountants (SAICA) (2016). *Protection of Personal Information Act.* Available from: https://www.saica.co.za/Technical/LegalandGovernance/Legislation/ProtectionofPersonalInformationAct/tabid/3335/language/en-ZA/Default.aspx. (Accessed on 1 August 2016).

Sanders, N.R. (2007). An empirical study of the impact of e-business technologies on organizational collaboration and performance. *Journal of Operations Management,* 25(6):1332-1347.

Scott, S. (2015). *Importance of technology in the workplace*. Available from: http://smallbusiness.chron.com/importance-technology-workplace-10607.html. (Accessed on 28 September 2016).

Shinn, S. (2012). The Intersection of Business & Technology. *Bized,* 11(6):18-23.

Standard Bank victim of R300m fraud in Japan. 2016. *Fin 24,* 23 May 2016. Available from: http://www.fin24.com/Companies/Financial-Services/standard-bank-victim-of-r300m-fraud-in-japan-20160523. (Accessed on 27 July 2016).

Strenk, F. (2013). Achieving competitive advantage through superior risk management. Available from: http://www.lockton.com/whitepapers/Achieving_Competitive_Advantage_Through_Superior_Risk_Management.pdf. (Accessed on 30 September 2016).

Toader, C., Brad, I., Radac, A.M. & Marin, D. (2010). Aspects regarding risk management in projects. *Scientific Papers Animal Science and Biotechnologies,* 43(2):454-457.

Tseng, S. (2008). The effects of information technology on knowledge management systems. *Expert Systems with Applications,* 35(1):150-160.

Valentine, E.L. & Stewart, G. (2013). The emerging role of the board of directors in enterprise business technology governance. *International Journal of Disclosure and Governance,* 10(4):346-362.

Van Zyl, A.S. (2013). Sustainability and integrated reporting in the South African corporate sector. *The International Business & Economics Research Journal (online),* 12(8):903-926. Available from: http://search.proquest.com/openview/6b66596af41ac5aec023ed5f7bd94d77/1?pq-origsite=gscholar (Accessed on 30 August 2016).

Wessels, P.L. (2006). The South African business environment in which accountants function and the role of information technology in the environment. *Meditari Accountancy Research,* 14(2):131-149.

Wong, T.S. (2016). *Computer Security Risks*. Available from: http://www.wong-sir.com/cit/social_impacts/computer_security_risks.htm. (Accessed on 25 September 2016).

Annexure A

IT Competence risk

This type of risk refers to the IT knowledge of the organisation's directors. The more directors who have knowledge of IT, the better the directors can understand IT's impact on the organisation's strategy and risk profile. At present, it would seem that the biggest risk is that most directors lack the required level of IT knowledge to fully understand and manage these risks (Parent & Reich, 2009:16). Despite the fact that an organisation's information assets can account for more than 50% of its capital spending, most boards are still in the dark in terms of understanding IT spending and strategy. This is due to the fact that very few of them comprehend the full extent of their organisation dependence on IT (Nolan & McFarlan, 2005:1).

IT Infrastructure risk

This risk refers to computers, networks, operating systems, applications and databases providing the organisation with IT assets. Threats in this category can be divided in two main groups, namely, internally sourced risks and externally sourced risks. The internal risks normally consist of system failure, technology failure or network failure. These kinds of threats have been the focal point of IT Risk Management for decades (Parent & Reich, 2009:16).

External risks refer to outside sources gaining access to the organisation's networks and systems. Some examples of outside threats include:

- Hacking, which is defined by Maillart and Sornette (2010:358) as breaking into an organisation's system to exploit information and use that information to make money. An example of hacking took place in May 2016 when thousands of credit cards from Standard Bank South Africa were compromised and a total of R 300 million was lost due to ATM fraud taking place in Japan. This was done by means of obtaining the card information digitally and then using it to make withdrawals with fictitious cards (Standard bank victim, 2016).

- Viruses, which are man-made computer programmes that infect a file or programme on one's computers. It replicates or spreads itself by infecting other programmes on the same computer (Pekker, 2010).
- Worms, which can be defined as man-made programmes that replicate themselves but are different to a virus insofar as worms do not infect other programmes on the computer, but themselves to other computers (Pekker, 2010).
- Spam, which according to the Oxford Dictionary (2016) can be defined as "irrelevant or unsolicited messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc.".).

When outside attackers do gain access to an organisation's system, they have access to confidential information and the ability to cripple the organisation's network or systems (Parent & Reich, 2009:144). This leads to yet another threat, namely, the contravention of the Protection of Personal Information Act no 4 of 2013 (POPI). The purpose of this Act is to protect personal information by public and private bodies. (SAICA: 2016).

IT Project risk

Project risk refers to the risk inherent in a new and specifically large project being undertaken. New IT projects, particularly those changing core processes of organisations, have the ability to completely destabilise operations and put them at risk (Parent & Reich, 2009:144). It is commonly known that the larger a project is the more risk it bears, therefore it is very important that before a new project is undertaken, the scope is clearly understood, there are adequate project management systems in place and management is kept up to date at the appropriate level to decide whether the project must continue. If the above are not enforced, the project could suffer unexpected delays and technical setbacks, causing massive write-downs in the organisation (Nolan & McFarlan, 2005:6-7).

IT Business Continuity risk

Most organisations put emergency measures in place after 9/11 (Nel, 2010:11). Chief Intelligence Officers (CIOs) of most organisations realised they have to decentralise some of their operations to minimise the impact of natural disasters or terrorism on their business operations (Parent & Reich, 2009:145). To further minimise Business Continuity risk, management should ensure the physical separation of data processing centres, the logical separation of duties, off-site data storage and recovery. A comprehensive Business Continuity Plan (BCP) should also be in place (Parent & Reich, 2009:145). Examples of IT business continuity risks can include, but are not limited to, malicious activities such as fraud, sabotage, vandalism, terrorism, natural disasters such as earthquakes, tornados, floods, hurricanes, fire or leaks and technical disasters such as loss of website and e-commerce capabilities, loss of internet access for extended periods of time, loss of power to keep IT and other operations equipment running and loss of email access or file / folder access (Nel, 2010:22).

IT Information /Security risk

Information / Security risk refers to the loss of data, non-compliance with anti-spamming legislation and privacy laws such as the POPI Act. Acts such as the POPI are aimed at ensuring that people's personal information is kept safe and that only data which is necessary for business processes is kept in an authorised manner (SAICA:2016). Organisations have the responsibility for ensuring that controls are in place to protect personal information from intrusion or unauthorised usage such as hacking (Parent & Reich, 2009:146).

Annexure B

Names of the companies in the population as at 7 September 2016

1. Anheuser-Busch InBev SA NV
2. British American Tob plc
3. SABMiller plc
4. Naspers Ltd -N-
5. Glencore plc
6. Compagnie Fin Richemont
7. BHP Billiton plc
8. Steinhoff Int Hldgs N.V.
9. FirstRand Ltd
10. Sasol Ltd
11. Vodacom Group Ltd
12. Standard Bank Group Ltd
13. MTN Group Ltd
14. Anglo American plc
15. Old Mutual plc
16. Aspen Pharmacare Hldgs Ltd
17. Mediclinic Int plc
18. Sanlam Ltd
19. Barclays Africa Group Ltd
20. Remgro Ltd
21. South32 Ltd
22. Anglo American Plat Ltd
23. Mondi plc
24. Shoprite Holdings Ltd
25. Nedbank Group Ltd
26. AngloGold Ashanti Ltd
27. BID Corporation Ltd
28. Hammerson plc
29. Woolworths Holdings Ltd
30. RMB Holdings Ltd
31. Discovery Ltd
32. Intu Properties plc
33. Tiger Brands Ltd
34. Growthpoint Prop Ltd
35. Capitec Bank Hldgs Ltd
36. Gold Fields Ltd

37. Rand Merchant Inv Hldgs Ltd
38. Reinet Investments S.C.A
39. Brait SE
40. Investec plc