An analysis of information technology risks and governance disclosure: Evidence from the top 40 JSE listed companies

By

TAURAYI STEPHEN NYAGOPE

221120330

Submitted in partial fulfilment of the requirements of the Master of Accountancy degree at the University of KwaZulu-Natal

Supervisor:

Professor Raj Rajaram

Co-supervisor:

Dr Oloyede Obagbuwa

2022

Declarations

I, Taurayi Stephen Nyagope, declare that:

a) the research reported in this dissertation, except where otherwise indicated, is my original research;

b) this dissertation has not been submitted for any degree or examination at this university or any other university;

c) this dissertation does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged;

d) this dissertation does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers;

e) where other written sources have been quoted, then:

(i) their words have been re-written, but the general information attributed to them has been referenced;

(ii) where their exact words have been used, their writing has been placed inside quotation marks, and referenced;

f) where I have reproduced a publication of which I am author, co-author or editor, I have indicated the part of the work I wrote alone and have fully referenced such publications;

g) this dissertation does not contain text, graphics or tables copied and pasted from the internet, unless specifically acknowledged, and the source detailed in the bibliography section.

Signed: *T.S. Nyagope* – (221120330) Date: 2 December 2022

Acknowledgements

I would like to express my appreciation to the following people for their contributions towards my thesis:

- God almighty for giving me strength and wisdom
- My wife and my daughter
- My brothers for being there for me the whole year and sending supportive messages.
- My supervisors Prof Raj Rajaram and Dr Oloyede Obagbuwa for their guidance and encouragement.
- The management from department, especially Professor Sibanda for guiding us on thesis writing.

Abstract

The study analysed the extent to which information technology risks and governance is disclosed by top 40 JSE-listed companies in their 2021 integrated reports as part of the risk governance practices. It also conducted a review to identify similarities and differences between King IV and other international standards such as ISO 27002, 38500, COBIT 5, SOX, and ISA 315 on IT governance and risk disclosure requirements. The results revealed that 32 out of the top 40 JSE-listed companies (80%) fully complied with King IV and other international standards on the disclosure of their IT governance and risk management in the integrated and corporate governance reports. The results further revealed that 8 out of the top 40 JSE-listed companies (20%) partially complied with King IV on disclosure of IT governance and risk management. Furthermore, the results indicated that King IV and other international standards were similar on 19 out 24 (79%) of the IT governance and risk management disclosure requirements and differed on 5 out of 24 (21%) requirements. The study confirmed the extent of IT and risk governance disclosure of the selected companies and determined areas of similarities and differences. The study adds to the debate on King IV disclosure requirements with regards to IT governance and risk management by public companies in corporate reporting and further adds to the debate on stakeholder theory.

Keywords: Information Technology; Risk Governance Disclosure; King IV

TABLE OF CONTENTS

List of Tables

List of Figures

List of abbreviations and Acronyms

Abbreviations:

ERM – Enterprise Risk Management

IR – Integrated Report

IASB – International Accounting Standards Board

IEC – International Electrotechnical Commission

ISACA – Information Systems Audit and Control Association

JSE – Johannesburg Stock Exchange

FTSE – Financial Times Stock Exchange

IT – Information Technology

ISO – International Organisation for Standardisation

IODSA – Institute of Directors South Africa

ISA – International Standards on Auditing

SOX – Sarbanes-Oxley Act

CEO – Chief Executive Officer

CIO – Chief Information Officer

COBIT – Control Objectives for Information Technologies

COSO – Committee of Sponsoring Organisation of the Treadway Commission

USA – United States of America

CHAPTER 1 INTRODUCTION & BACKGROUND

1.1 Introduction

Information Technology (IT) has become an integral part of modern entities. The use of IT systems has resulted in quicker business communication, large space for electronic data storage, protection of data, accelerated data processing and efficient connection of business processes with other businesses in real time. In modern entities, IT equipment is present everywhere; in offices, factories, schools, business processes and this has led to the rapid change in behaviour and communication of companies and individuals (Jusufi, 2013). The use of computer application systems by business has brought many benefits that increased productivity and efficiency, but it also brought with it significant risks that can impact a business's ability to operate as a going concern (Marx & Hohls-du Preez, 2017). The successes of organisations can be linked to those companies which have aggressively adopted IT systems. IT systems and technologies are however constantly changing, which therefore requires companies to keep well-informed of these changes (Hohls-du Preez, 2016). IT, risk management, and governance play a vital role in companies' alignment of objectives to the strategic vision as well as achievement of business objectives (Pirta & Strazdina, 2012). The use of IT application systems assists management with seamless efficiency in business processes and decision making. Artificial intelligence has further increased the use of IT application systems and plays a significant role in an organisation's operations as well as its annual financial reporting. Furthermore, the use of IT application systems has resulted in improved reliability of financial reports, as transactions are processed with uniformity, hence eliminating the risks of errors which mainly take place in manual systems (Ngwenya, 2015). The increased use of IT application systems has also exposed companies to sophisticated risks, which can potentially harm the company's going concern (Marx & Hohls-du Preez, 2017).

Effective IT controls should be taken into account to guarantee that IT risks are reduced to an appropriate level and to ensure accuracy and reliability of financial reporting (Pirta & Strazdina, 2012). Effective IT systems ensure constant communication and increase reliability on delivery of goods and services. A company's implementation of effective corporate governance on IT and IT risks will reduce/eliminate the IT risks it is exposed to through technology applications (Pirta & Strazdina, 2012). Management should ensure that policies and procedures on IT governance, including IT risk assessment, are put in place and should be followed. To ensure good governance practices, codes of corporate governance were designed,

ranging from King I, which was effective in 1994, to King II, which replaced King I and became effective in 2002, King III which replaced previous King codes and became effective in 2009, and King IV, which was effective from 2017. These were designed to respond to the rising concerns of corporate governance failures and hence the need for the King IV (IoD, 2016). The King IV principles and recommended practices include Information Technology (IT) governance and risk management application disclosure as one of its key elements, designed with the primary purpose of promoting the effective and efficient use of IT application systems.

The main aim of this study was to analyse the extent to which IT governance and risk disclosed in the 2021 annual reports of JSE's top 40 listed entities are consistent with King IV corporate governance and other international standards including ISOs and ISA 315. It also further sought to ascertain whether IT risks are included in the integrated reports and whether appropriate explanation of the information is made. The study is relevant as it adds to literature on company compliance with IT governance and risk disclosure as per the King IV.

1.2 Background to the study

The board of directors, which is constituted by those charged with governance, is expected to govern IT application systems in a manner that will assist a company to achieve its strategic objectives (IoD, 2016). Furthermore, the board of directors is expected to manage company's risks in a way that supports an organisation's operations to enable it to achieve its strategic objectives (IoD, 2016). Information Technology is a critical component of risk management and governance which helps the board of directors and executive management to identify and address IT risks for a company. The use of information and technology systems plays a vital role in various business processes, which include data capturing, data processing, data communication, preparation of financial reports, and technology internal controls on different levels. IT application systems have resulted in data development and electronic processing of many transactions (Ngwenya, 2015). IT applications are used for the electronic processing of data, and this may expose companies to different risks. Electronic data processing and transactions have exposed company operations to significant risks, which in turn requires organisations to develop internal controls aimed at reducing the risks. These controls should be designed to ensure that risks a company is exposed to in using IT will be mitigated. Adoption of IT systems has transformed the nature of global communications, changing business

processes internally among various company departments as well as externally with all its stakeholders (Ramamoorti & Weidenmier, 2004). The use of IT application systems in business operations has increased significantly over the years. Companies have embraced the use of information technology to keep their aggressive side in the market environment, ensure productivity and business process improvement, and increase cost efficiency and revenue growth (Marx et al., 2016). IT application systems have accelerated data processing, resulting in companies achieving multiple tasks/performance targets over a shorter period (Alkebsi et al., 2014). The adoption of IT application systems by companies has also resulted in a significant decrease in errors, hence an increase in accuracy in the processing of large volumes of data (Alkebsi & Aziz, 2017). The use of IT application systems enhances the reliability of financial information, uniformity of transaction processing, and elimination of human errors which are most common in manual systems. IT application systems have acted as the primary enabler and facilitator of efficient business processes in companies. It has therefore become important for companies to implement IT governance to ensure the reliability and availability of not only IT systems, but also financial information obtained from the operating systems which are used to support the company (Jordaan, 2019). Information technology has exposed companies to new risks which have threatened their continued existence as a result of IT systems failures; therefore, governance and security are critical to efficient business processes. Furthermore, increased adoption of technology, data, and communication integration and usage have led to sophisticated risks, including cybercrime (Jordaan, 2019).

IT governance is the ability of those charged with governance, together with senior management, to measure, direct, and evaluate the organisation's use of IT resources to achieve its strategic objectives (IoD, 2016). According to Brisebois et al. (2007), the board of directors should review IT governance based on value addition to the company and its ability to meet its strategic objectives and good governance. The King IV code of corporate governance was designed and introduced in 2016 and it became effective in April 2017 as an addition to the existing King I, II and III codes (IoD, 2016). The code functions to set up the principles and guidelines to be applied by entities to achieve good governance (IoDSA, 2018). Compliance with the King Code by entities is voluntary; however, it is a mandatory requirement for all JSE-listed entities to comply with and report on King IV (JSE, 2017).

Increased use of IT application systems has exposed companies to more sophisticated risks in their operations. Good governance and effective management of information and technology and all other risks are vital for success of an organisation. In addressing these IT-related risks, management is required to exercise their duties to manage these risks in a manner that assists an organisation to design and achieve its main objectives (IoD, 2016). Information technology risk governance disclosures are therefore essential for a company as they assist stakeholders who use the integrated reports and financial reports to have a clear insight of the risks that entities are exposed to and measures that are in place and which management has implemented to minimise these risks. Companies worldwide have significantly adopted the use of IT application systems to ensure accuracy, efficiency, and effectiveness. The use of the technology contributes positively to an organisation's operations; however, it also comes with significant threats. It is therefore regarded as a significant area of study as IT and its risks pose a threat to a company's existence as a going concern.

King IV provides guidelines and outlines the importance of IT governance and risk disclosures, which assist stakeholders/users of annual financial statements to assess risks and make informed decisions. King reports were designed to promote corporate governance by companies operating in South Africa, and mainly those listed and the non-listed on JSE. JSE mandated all listed entities to follow all the corporate governance principles outlined in the King IV Code, including IT governance (JSE, 2022). Disclosure of IT and risk governance practices has been regarded a litmus test for listed companies and has become a very significant element of corporate governance (IoD, 2016). IT governance and risk management disclosures are an important part of corporate governance (Madrigal et al., 2015).

There is extant literature assessing the IT governance and risk disclosure compliance with King II and King III; however, the extent to which organisations are conforming to the King IV's principles on IT and risk governance disclosure requirements is unknown. The existing research confirms that disclosure of IT governance and risks provides stakeholders and investors with some assurance and confidence in a company. It is therefore important that stakeholders and investors are well informed of the company's IT and information systems governance and risks to make their economic decisions. This study therefore analysed, examined, and assessed the compliance of the top 40 JSE listed entities with King IV on IT governance and risk disclosures.

The study sought to analyse whether IT risks and governance have been properly disclosed and effectively managed to ensure the company's continued existence. The study focused on companies listed on the JSE because compliance with King IV principles and recommended practices is mandatory for them. Non-compliance with the King IV governance principles may lead to JSE suspending an entity's listing, which, therefore, makes it very important to assess the extent of entities' compliance. This study specifically explored the top 40 largest entities listed on the JSE. The top 40 entities listed on the JSE constitute 80% of the total market capitalisation (Baker et al., 2016; Barr et al., 2007; Kotze, 2017; Marx & Mohammadali-Haji, 2014; Marx & Voogt, 2010; Pholohane et al., 2020); thus, the study was a fair representation of the total companies listed on the JSE.

1.3 Research Problem

Information technology risks place an entity's going concerns and its continued operations at great risk. Furthermore, an entity's compliance with IT and risk governance is considered a vital tool to enhance its operations and existence into the near future. IT governance and its related risks have a direct impact on the ability of a company to continue, as these risks affect the smooth running of IT systems and data within the system. The going concern risk posed by IT risk in business is problematic, and lack of IT governance and risk disclosure compliance with King IV by those charged with governance will further increase the risk of non-compliances by an organisation. Failure of IT governance exposes a company to extensive financial loss as well as loss of key information, which can lead to extensive reputational damage, legal exposures, and loss of stakeholder confidence. IT governance failure has an adverse effect on the company's performance and is likely to impact investors and stakeholders' decisions. It is therefore important to determine the extent of compliance by organisations to IT and risk governance disclosure requirements as per King IV.

1.4 Objective of the study

The study aimed at addressing primary and secondary objectives listed below:

1.4.1 Primary Objective

The primary objective of the research paper was to assess the extent of compliance by the JSE top 40 listed entities with King IV on IT and risk governance disclosures. Furthermore, the study seeks to analyse the similarities and differences between King IV and other international standards on IT & risk governance disclosure requirements.

1.4.2 Secondary Objectives

The study was aimed at achieving the following secondary objectives:

i. Assessing the extent to which the JSE top 40 listed entities comply with King IV on IT and risk governance disclosure requirements in their integrated annual reports and corporate governance reports.
ii. Determining the IT governance and risk disclosure requirements in accordance with King IV and other international standards such as International Organisation for Standardisation (ISO 38500), Sarbanes-Oxley Act (SOX), and International Standards of Auditing 315 (ISA 315).
iii. Providing recommendations to King IV IT governance and risk disclosure following the international standards (ISO 38500 & COBIT 5), Sarbanes-Oxley Act (SOX), and ISA 315 on disclosure requirements for South African companies that are required to comply with King IV.

1.5 The Research Questions

The research was undertaken with the main aim of providing answers to the research questions and exploring empirical research to solve the obvious research problem. The following research questions were used:

(a) To what extent are the JSE top 40 listed entities complying with King IV and other international standards on IT governance and risk disclosure requirements?
(b) What are the similarities and differences between King IV, International Organisations for Standards (ISO 38500 & COBIT 5), Sarbanes-Oxley Act, and International Standards of Auditing 315 in terms of IT governance and risk disclosure requirements?
(c) What are the likely recommendations regarding IT governance and risk disclosure that will enhance King IV provisions?

1.6 Contribution to Literature

The study is one of the few studies conducted on King-IV which was recently developed from the previous versions (King I to King III). The study provides empirical results on the JSE top 40 listed companies' compliance with King IV on IT governance and risks management disclosure requirements. There are notable studies that were done on assessing the company's compliance with IT governance/risk disclosure requirements in accordance with King II (Janse van Vuuren, 2006) and King III (Ngwenya, 2015), but there is little to no study identified in

literature which focused on entities' compliance with IT governance/risk disclosures as required by King IV. This study adds to the work of Janse van Vuuren (2006) and Ngwenya (2015) by examining, assessing, and evaluating the compliance of the top 40 listed entities with King IV requirements on IT governance and risk disclosure. The top 40 entities listed on JSE constitute 80% of the total market capitalisation, making the study a fair representation of the total companies listed on JSE (Baker et al., 2016; Barr et al., 2007; Kotze, 2017; Marx & Mohammadali-Haji, 2014; Marx & Voogt, 2010; Pholohane et al., 2020).

1.7 Significance of the study

This research is significant as it potentially assists the authors of King IV code in clarifying the IT governance and risk disclosures by JSE listed entities. The disclosure results/findings are beneficial to stakeholders and investors as IT governance is an important factor to be considered before undertaking an investment. Good governance is known as the ability to exercise ethical and effective leadership by management and board for the primary purpose of achieving the entity's objectives of good performance, effective application of controls risk management, and financial reporting (IoD, 2016). Users significantly place reliance mainly on the entity's annual financial reports and corporate governance reports to inform them on the application of corporate governance practices within a company.

The stakeholders include company regulators, policy and standard setters, investors, shareholders, employees, and Johannesburg Stock Exchange (JSE) among others. The study is significant as it is going to assess and analyse how the JSE top 40 listed entities are complying with King IV corporate governance disclosures, mainly on IT and risk governance. Effective corporate governance practices on IT governance and risk will enable companies to reduce the risk of going concern, which will benefit the employees with guaranteed employment, shareholders and potential investors with guaranteed returns, and the South African economy through company contributions in the form of taxation to government. JSE's top 40 listed entities constitute the largest market share in the capital markets; therefore, the study will be of high importance to company regulators including the Johannesburg Stock Exchange, as it can be used to deal with companies that will be identified to be non-complying to King IV corporate governance. The study is going to be useful to company regulators, policy makers, investors, shareholders, and other stakeholders, as it will provide them with the state of compliance and non-compliance on King IV corporate governance disclosures on the listed

companies in South Africa. This study is important because it can be used by standard setters to assess the compliance status of listed companies in their application of King IV governance practices. The findings of this study will help the South African Institute of Directors clarify current disclosure compliance with King IV, which can be used in the development of other codes of governance reports in the future.

1.8 Limitations of the Study

There are limitations to this study as it focused only on the top 40 listed entities on the Johannesburg Stock Exchange (JSE) and thus may not be a full representation of the total entities. Furthermore, compliance with King IV disclosures is a mandatory requirement for companies listed on JSE whilst it is a voluntary requirement for non-listed companies, which adds further limitations as the study only focused on listed companies and ignored the non-listed companies. However, the main reason for including only the top 40 JSE listed entities as the total population for this study is that these entities constitute over 80% market value of all companies listed on JSE (Baker et al., 2016; Pholohane et al., 2020). An assumption was made that if JSE's top 40 listed entities adhere to King IV IT governance and risk disclosure, other companies including smaller and unlisted companies will also follow. All the top 40 listed entities were included in the empirical study. The study used King IV as a corporate governance framework recommending the best practices for effective IT and risk governance and risk management. Significant improvements have been made, from King III's "Apply or Explain" approach, which often resulted in a "tick box" exercise, to King IV's "Apply and Explain" outcome-based philosophy. However, King IV provides guidelines and lacks statutory power to enforce adoption and disclosure, thus solely relying on other statutory bodies to enforce its principles and recommended practises.

1.9 Organisation of the study

This part summaries the structure of the study and how it was carried out from the start to finish. The study report comprises of the following chapters:

Chapter 1: Introduction and background

This chapter presents the introduction, background of the study, research problem, primary and secondary objectives, research questions, significance of the study, and the contributions of the research to the literature.

Chapter 2: Literature review

This chapter examines literature on theoretical and empirical studies. Furthermore, it also provides a synopsis of King IV and other international standards on IT & risks governance disclosure requirements including ISO 38500, 27000, 27001, 27002 COBIT 5, SOX, and ISA 315.

Chapter 3: Research methodology and research design

This section provides a detailed explanation of the research methodology of the study, including its rationale and relevance. Also, the data collection methods are discussed in this chapter.

Chapter 4: Data presentation, analysis, results, including findings

This chapter presents the analysis, results and findings on the extent to which JSE top 40 listed entities comply with King IV's risk disclosure and IT governance requirements. It further presents the research results on the similarities and differences of King IV with other International Standards on IT governance and risk disclosures.

Chapter 5: Summary and conclusion

The chapter focuses on providing a summary of the study, findings and implications of findings identified. Furthermore, study findings, a summary of the similarities and differences, limitations and suggestions for future areas of study based on identified research gaps are discussed in this chapter. The chapter also covers conclusions on the identified differences between King IV used in South Africa and other international standards on information technology and risk governance disclosure. A summary of similarities and differences identified between King IV and other International Standards on IT governance and risk disclosure requirements is given.

1.10 Chapter Summary

It is important to note that information technology plays a vital role in the success of an organisation. However ineffective IT governance and risk management exposes organisations to different types of risks which can threaten their going concern ability. It therefore requires organisations to implement effective controls over IT governance to make sure that IT risks are decreased to a satisfactory level, thus ensuring reliability of financial reports. Disclosure of IT risks and how such risks are managed, and IT governance are important for all stakeholders as the enable them to make informed decisions. The study analyses the level of IT and governance risks disclosed in the annual reports of the top 40 JSE-listed entities.

The following chapter reviews literature review on IT governance and risk disclosure, mainly focusing on the stakeholder theory, IT, IT governance, IT risks and IT governance and risk disclosures of King IV and other standards.

CHAPTER 2 LITERATURE REVIEW

2.1 Introduction

The main aim of the section is to review existing research studies to identify those that are relevant to the current study and to identify gaps in existing research. This review on existing studies includes a review of published and unpublished research papers, internet searches, books, and articles. Internet searches, university library resources and archives will be utilised to identify the existing literature. As the study background, problem statement and study objectives were clearly outlined in chapter one, the theory underpinning this study and other elements on IT and IT governance are discussed in this chapter. There are several theories which have been used to analyse company disclosure. This study used stakeholder theory in understanding and analysing company motivations to disclose risks in company annual reports. Stakeholder theory is explored in this chapter, followed by literature on JSE top 40 listed entities, integrated reporting/corporate governance reporting, information technology, IT risks, IT governance, King IV and other international standards disclosure requirements on IT governance and risks, JSE top 40 listed entities' acquiescence with the King IV and international standards IT governance/risk disclosure requirements, and comparison of IT governance & risk disclosure requirements of King IV with those of other international standards. The literature review follows the flow presented in figure 2.1.

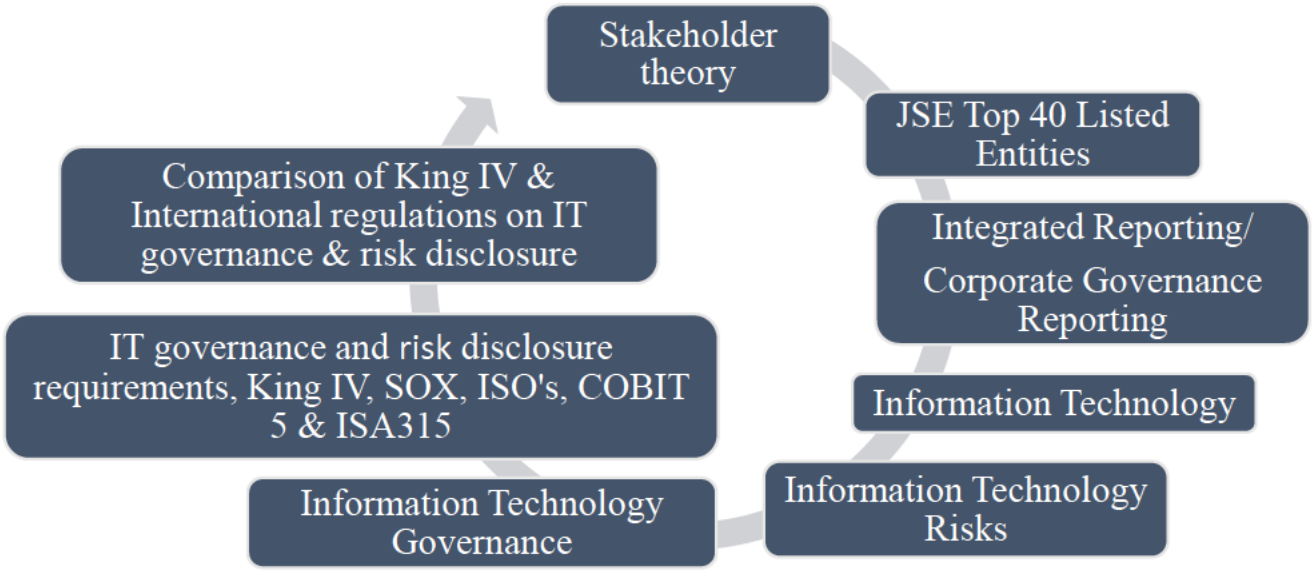


Figure 2.1: Flow of Literature

Source: Designed by the researcher

Figure 2.1 presents the flow to which literature review will be followed. This will enable the researcher to link the existing literature to the current study.

2.2 Theoretical Framework

To contextualise this study, stakeholder theory was used. Abraham and Shrives (2014) define stakeholder theory as a way in which companies make voluntary disclosures including IT governance and risks to manage stakeholder activities as well as improve corporate governance and disclosure. Companies thus attempt to disclose financial and non-financial information to influence their stakeholders' perceptions. The stakeholder theory is discussed below.

2.2.1 Stakeholder Theory

According to the stakeholder theory, companies make voluntary disclosures as a way to manage stakeholders attention and improve corporate governance and disclosure (Abraham & Shrives, 2014; Boesso & Kumar, 2007). Stakeholders interested in corporate information include shareholders and investors, as well as other groups interested in corporate information (Madrigal et al., 2015). According to Boesso and Kumar (2007), the more important a stakeholder is to a company, the greater the expected influence it has on a company's disclosure exercises. In addition, companies pay more attention to key stakeholders who may directly or indirectly influence their operations and disclosure of information (Madrigal et al., 2015).

A stakeholder is known as any individual or a party that has interest or can affect or be affected when a company achieves its strategic objectives (Freeman & Reed, 1983). Stakeholders can be viewed in a wider sense and in a narrow sense. A wider sense stakeholder is known as any individual or group who can affect the accomplishment of an entity's objectives or are affected by the accomplishment of an entity's objectives, whereas a narrow sense stakeholder is an individual or group on which an entity is dependent for its continued existence (Freeman & Reed, 1983). Stakeholders are groups or individuals whose rights should be respected and not violated through the company's actions (Castelo Branco & Lima Rodriques, 2007). Examples of stakeholders who are influenced are shareholders, investors, suppliers, customers, regulatory authorities, employees, communities, environment and future generations (Freeman & Reed, 1983).

Stakeholder theory is one of the tools that provide guidance on how management operates as compared to addressing management theorists and economists (Freeman & Reed, 1983). Stakeholder theory generally addresses the broader interests of society, recognising that many stakeholders who are affected by decisions and the nature of their relationships are important. With stakeholder theory, a firm should consider the interests of all parties affected by its actions

(Rossouw, 2005). According to stakeholder theory, organisations have a social duty and should consider the interests of all parties affected by their actions (Castelo Branco & Lima Rodriques, 2007). The South African Institute of Directors (2016), supports the stakeholder theory through the six internationally accepted King IV key governance principles which include discipline, fairness, transparency, accountability, independence, and social responsibility to all stakeholders and not only shareholders (Mariri & Chipunza, 2011).

Stakeholder theory can be described using two main questions (Freeman & Reed, 1983). The first question relates to firm purpose. This question is aimed at encouraging management to convey the shared sense of value they create, and what brings its stakeholders together (Freeman et al., 2004). The second question relates to management's responsibilities to the company's stakeholders. This allows management to describe how they will run an entity including the kind of relationships with stakeholders needed to achieve the entity's objectives (Freeman et al., 2004). The two questions above are aimed at ensuring that management articulate the shared sense of value which is created in the company, and what brings the company's stakeholders together (Freeman & Reed, 1983). The three categories of stakeholder theory are normative, instrumental, and descriptive (Donaldson & Preston, 1995), and these are described below.

Descriptive: The descriptive stakeholder theory category explains the concepts of a company, their operations, and their environmental implications. According to Donaldson and Preston (1995), a company is defined as a group of mutually beneficial and competing pursuits which create value. Descriptive stakeholder theory category is used to define the nature and operations of an entity, how it is managed, how management and board of directors think about the entity and its stakeholders (Donaldson & Preston, 1995). The descriptive stakeholder theory explains the actual behaviour of managers, entities and stakeholders (Obalola, 2008).

Instrumental: The instrumental stakeholder theory is useful in that it helps in managing stakeholders, and this will result in the company achieving its goals, which include profitability, growth, and sustainability. The instrumental stakeholder theory enables the assessment of the connection between stakeholder management and achievement company goals (Donaldson & Preston, 1995). Instrumental stakeholder theory suggests stakeholder goal oriented solutions such as how managers should achieve an entity's specific objectives, which may or may not have ethical considerations (Hendry, 2001). Instrumental stakeholder theory

demonstrates the entity's pursuit of its interests, through managing its relationship with other stakeholder groups (Obalola, 2008).

Normative: According to Donaldson and Preston (1995), normative stakeholder theory category acknowledges that stakeholders have legitimate interests which integrate activities based on their interest in the company. It gives room for forecasts, and assists in providing suggestions and recommendations, which support stakeholder management (Donaldson & Preston, 1995). Normative theory requires management to act in the interest of the stakeholders and the entity to ensure its survival and safeguarding the long term benefits of all parties (Hendry, 2001). Stakeholders enjoy a normative status, and not simply instrumental status (Rossouw, 2005). Normative stakeholder theory addresses the moral duties of an entity's management of its stakeholders. The normative approach to stakeholder theory entails that stakeholder needs should not only be recognised for influential or tactical purposes, but should also be as a result of moral obligations (Obalola, 2008). The stakeholder theory requires entities to consider social responsibility initiatives in the communities and amongst parties interested and affected by the entities' operations. Therefore, it is important for entities to make decisions that include social responsibility, which links corporate governance and financial performance (Mariri & Chipunza, 2011).

It is clear how companies use their disclosures in the integrated and annual reports to influence and manage their stakeholders, a technique that made using stakeholder theory appropriate in this study. This stakeholder influence through corporate disclosures is explored in this study mainly in the area of IT governance and risks. An entity's disclosure of its IT governance and risks is very important to the stakeholders, who are not only limited to shareholders or investors, to assess the entity's ability to maximise the use of IT applications to increase operating efficiency and minimising risks exposed. As part of its important concepts, King IV suggests that a company should implement a stakeholder-inclusive approach which considers the interests of the company and its stakeholders a priority compared to the rights and needs of shareholders. Stakeholders use disclosures to assess risks and opportunities before investing in an entity, and this all points to the importance of corporate disclosures to stakeholders. To make economic decisions, stakeholders rely on information disclosed by entities in the annual reports and integrated reports. This means that an entity's compliance with King IV disclosure requirements on IT governance and risks is important to stakeholders. The mandatory requirement of JSE listed entities to disclose is also stakeholder oriented.

2.3 Conceptual Framework

The use of IT resources enabled entities to easily adapt to changes with developments as well as gaining a competitive advantage over its competitors. However, the adoption of these IT application systems has exposed them to various IT related risks which include strategic risks, financial risks, operational risks and technological risks (Ngwenya, 2015; Pa et al., 2015). To ensure effective monitoring and control of these risks, IT governance, risk management and risk assessment policies and strategies have to be in place to control the use IT systems aimed at achieving an organisation's objectives (Ngwenya, 2015). IT governance has thus been used to effectively manage, monitor, and control the risks entities are exposed to as a result of using IT applications (Ngwenya, 2015). Levstek et al. (2018) define IT governance as the fundamental decision-making process in the IT arena, focusing on the provision of decision rights and responsibilities for the effective use of IT systems as well as strategic alignment between IT and an entity's operations aimed at creating value. Information technology governance and risk management are an effective collaboration tool used to control risks and information within a company.

IT governance and risk management advocates for responsible management to improve the availability of IT resources which include IT applications systems, information and infrastructure to achieve governance and control (De Haes & Van Grembergen, 2008). IT application systems constitute an important tool to an organisation as it supports growth and sustainability. IT governance and risks management is the duty of the board of directors and senior management and consists of leadership, organisational structure and processes to ensure that IT applications are utilised to achieve an entity's strategy and objectives (De Haes et al., 2017). IT governance and risks management is vital for safeguarding stakeholders, assets and an organisation's confidential information, reputation, trust and an organisation's brand. Companies disclose their IT governance and risks with the aim of ensuring that stakeholders are informed on how its risks are effectively managed, hence influencing their decisions. The disclosure of information relating to IT governance and risks is a JSE listing and King IV mandatory requirement, as investors and other stakeholders use the disclosure to assess risks and potential opportunities when making economic decisions.

2.4 Empirical Study

2.4.1 Information Technology (IT)

Information technology has become a critical resource for all companies; it plays a critically important role in the collection and processing of information, its availability to support business decisions and strategic objectives (Mangalaraj et al., 2014). The ongoing industrial revolution ($1^{st} – 4^{th}$) has resulted in growth of IT adoption in company activities and has given rise to the adoption of IT use in financial reporting and auditing (Byrnes et al., 2012). The most considered development in the space of IT has been the internet, which has completely removed international boundaries and created an instant world (Hohls-du Preez, 2016). Internet has brought the world closer together where information is shared and distributed in real time, and where the use of internet allows the exchange of information between different parties, for example between buyers and sellers, service providers and customers (Hohls-du Preez, 2016). IT is regarded as the most important pillar for an organisation's success and hence influences how an organisation creates value, thus creating a competitive advantage (Elazhary et al., 2022). IT use led to an increase in the quality, accuracy and speed of organisational processes, thus increasing efficiency and effectiveness in the provision of goods and services to customers (Tohidi, 2011). Information and technology cuts across all mechanisms and processes in an organisation and is therefore considered not only an operational enabler but also an important asset. As a strategic asset of an organisation, IT should be governed and controlled to ensure that it supports the organisation to meet its strategic objectives (Hohls-du Preez, 2016). With the adoption of IT, organisations strives to minimise the cost of IT, maintains IT risks to lower levels and complies to regulations and laws on the use of IT (Mangalaraj et al., 2014).

Information and Technology (IT) plays the most vital role in a company's operations. From small medium enterprise to large companies, IT systems management is one of the major responsibility of those charged with governance (O'Brien, 1996). IT use has resulted in increased efficiency on company's operations and increased opportunities for innovations through exploiting all IT systems aimed at achieving company's goals in a more simplified manner (Moolman & Ngwenya). The use of IT systems in company's operations has improved the internal controls systems in the business environment and significantly reduced information processing time, errors and achievement of multiple objectives (Alkebsi et al., 2014). Effective use of IT results in quicker and reliable delivery of services, communication, and other

products. The adoption of IT has accelerated data processing, and which resulted in a rapid achievement multiple tasks/objective (Alkebsi et al., 2014).

By using IT tools, a company can convert information in a more comprehensible, more attractive, and more useful format (Curtin, 1998). Companies using technologically advanced tools gains a competitive advantage in its operations. Companies have moved from the use of traditional methods to IT methods, and this has resulted in more efficient operations and provided an improvement in communication within the entity and between the entities and its stakeholders. The use of IT systems has exposed companies to new risks which require effective IT risk management governance strategies by companies (Curtin, 1998). The development of IT over the years has brought significant benefits to companies, however with these developments, the use of IT exposed companies to significant new risks. These risks that companies are exposed because of IT systems usage are discussed in the next section.

2.4.2 Information Technology Risks

According to Marx (2009), IT risk is defined as the likelihood that a certain threat will affect information system processing and have a significant effect on an entity's operations. IT risks also involve to events or actions that may result in a loss or damage to software application systems, hardware components, and data or information (Marx, 2009). Information technology risks can also be defined as all events or actions that can cause a loss or damage to computer hardware, software, data or information (Hohls-du Preez, 2016). These risks may arise due to, unlawful disclosure, changes, or damage of data, accidental errors and exclusions, IT-related interruptions, which are unintentional or because of mistakes and lack of professional due care in the execution and processing of the information (Parent & Reich, 2009).The rapid growth of e-commerce and business activities has increased reliance on IT resources, which has exposed businesses to many significant risks, challenges and threats which includes cyber security, hacking, going concern among others (Marx, 2009; Schutte & Marx, 2018). Furthermore, the board of directors and executive management has the responsibility to inform the stakeholders of the IT related risks which an organisation may be exposed to, and how these can affect the company. Effective application of IT governance reduces the IT related risks and disclosure of these risks in the integrated reports becomes critical as it enables stakeholders to understand how IT resources are effectively used and how IT risks are monitored and controlled to achieve the organisations' strategic objectives.

Marx and Hohls-du Preez (2017); Parent and Reich (2009); (Schutte & Marx, 2018), identified some of the IT risk which are exposed to organisations as a result of using IT application systems in their operations, and some of these includes;

- IT Competence risks which mainly relates to the IT expertise of the board and executive management of a company;
- IT Governance risks which relate to the failure by the board of directors to apply the IT governance principles as stipulated in King IV code which can result in reputational damage, loss of investor and stakeholder confidence as well as listing for entities listed on JSE;
- IT Infrastructure risks which are primarily related to risks on facilities and infrastructure used by a company which includes among others computer, networks, operating systems, software systems and databases systems do not function in the manner indented by management;
- IT Business continuity risks which mainly relates to a company being unable to operate due to disasters and resulting in loss of critical information;
- Data security risks that mainly relates to unapproved users obtaining access to company's important and protected information which may result in loss of data;
- Project risks which are mainly risks associated with new projects undertaken by an organisation related to IT;
- IT access risks which relate to risk of exposure of an organisation's confidential or sensitive information to unauthorised users;
- IT integrity risks which relate to unreliable data due to inaccuracy or incomplete;
- Disruptions on IT systems which may result in loss of information and data as well as organisation's operations and continuity;
- IT failure which can lead to loss of key information and data;
- Cloud computing – organisations have increased the use of cloud computing mainly for data storage and this have exposed them to risks of information loss, interruption of services due to reliance of third-party services providers operating and maintaining the cloud space;
- Social networking risks which are mainly exposed to organisations as a result of using social media technology and these includes risk of brand and legal violations which may negatively affect an organisation's reputation;
- Malware computer virus increases the risks of loss of information and loss due to corruption of the organisation hardware which results in loss of production;
- Cyber-attacks which are more complex and often exposed to organisations with more adverse effects including financial fraud, money laundering;

- Data breaches and unauthorised access to IT systems and confidential information which may result in contravention of the Protection of Personal Information Act (POPI) and
- Ineffective/ inappropriate alignment of IT systems to support the organisations processes.

It is extremely important for organisations to inform their stakeholders and investors about the risks they face when using IT applications and how these risks can affect the organisations' operations as well as how these can be managed effectively. The study therefore sought to assess if these risks to which entities are exposed to in using IT applications are disclosed in the integrated reports and governance reports aimed at providing stakeholders and investors with information which enables them to make investment decisions. Non-disclosure of the risks exposed to entities constitute a governance failure by the board and executive management and may lead to non-compliance on JSE listing requirements as well as the King IV's apply and explain code of corporate governance.

2.4.3 Information Technology Governance

IT governance is a process which involves evaluating, assessing and directing an organisations' plans to use IT systems and resources to support it to achieve its objectives whilst mitigating risks associated with the use of IT resources (Pa et al., 2015; Selig, 2018). According to De Haes and Van Grembergen (2008), IT governance is defined as management of company IT operations, processes and systems aimed at ensuring that these IT systems help businesses achieve their strategies and goals. De Haes et al. (2017) noted that an entity's governance of IT is an important part of corporate governance exercised by the board of directors and addresses the implementation of processes, structures and interactive mechanisms which enables both entity and IT personnel to execute their responsibilities to create value and achieve the entity's objectives. In addition IT governance is more focused on the management and the use of IT resources to achieve organisation's goals and therefore should not be viewed in isolation as IT is connected with other assets (Pa et al., 2015). Furthermore, IT governance is also known as an accountability framework that can be used to foster a desirable behaviour in using IT application systems in company (Juiz et al., 2014). IT risk governance is a process which enables companies to implement innovative business updates and investment in IT systems to adapt to changes, focuses on IT alignment, IT resources management, risk management and performance measurement (Pa et al., 2015).

IT governance is part of the responsibility of the board of directors and senior management team. It is an important part of a company's governance systems which comprises of the leadership, company structures and processes that are aimed at ensuring that IT supports the company's strategy and objectives. The company's board of directors and management team are responsible for directing the activities including controlling the design and execution of IT plan and objectives and ensuring the integration of company's operations with IT systems (De Haes & Van Grembergen, 2008). The main aim of IT governance is to direct IT activities to support an entity's operations and minimising IT risks, thus ensuring that it meets the company's strategy and objectives (Pa et al., 2015). IT governance is also aimed at ensuring that IT operating systems are aligned with the company's strategic objectives as well as to meet the IT governance risk disclosure requirements (IoD, 2016). IT governance is an important element in a business operations as it enables an organisation to direct its IT application systems to ensure that it creates and deliver value to the business at the same time mitigating risks which are exposed to the organisation by these IT systems (Rubino et al., 2017). IT governance is vital as it ensures that IT goals are aligned to the objectives of the entity as well as mitigating IT risks (Levstek et al., 2018). Effective IT governance contributes to an entity's performance and efficiency which includes increased reputation, trust and lower production costs (Levstek et al., 2018). In addition, IT governance offers an outline that enables entities to leverage their IT capability and manage their innovative practises (Elazhary et al., 2022). Researchers have noted that entities with more effective IT governance reflected significant increase in overall profits and hence effective governance of IT is considered the most important determinant of IT business value (Elazhary et al., 2022; Zhen et al., 2021).

The adoption of IT systems by companies has exposed them to number of risks that require effective management and control to ensure that IT systems support a company's objectives. Risk management and governance includes a process of identifying IT risks exposed to companies and establishing internal control systems to reduce these risks (Brisebois et al., 2007). The fundamental objective of IT governance is to ensure that the development and execution of IT systems in a company adds value and reduce the IT risks to an acceptable level (Brisebois et al., 2007). The IT governance enables the executive management and reduce any identified IT risks exposed to the company. Risk management is the cornerstone of IT governance, as it ensures that a company's strategic objectives are not put at risk by IT failures (Hardy, 2005). The following are general responsibilities of IT governance to the board and executive management (IoD, 2016);

- To align IT application systems with the company's strategic mission, direction,
- To align IT investments,
- To create an IT funding model for all the IT expenditures in by the company,
- To ensure IT delivers on its plans,
- To manage risks exposed to the entity because of using IT resources,
- To ensure improved customer services with the use IT applications.
- To ensure efficient utilisation of resources and assets,
- To create IT standards and support services aimed at assisting a company to achieve its strategic objectives and,
- To manage processing and the use of company information.

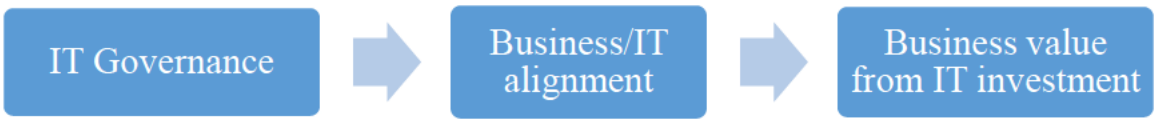


Figure 2.2: IT Governance definition

Source: *Levstek et al. (2018, p. 292)*

As indicated in figure 2.2, IT governance enables both the entity and IT personnel to execute their responsibilities to support business/IT alignment and the creation of value from IT-enabled business investment (De Haes & Van Grembergen, 2015; Haes & Grembergen, 2015). IT governance mechanisms plays a vital role through providing IT strategic direction aimed at ensuring the realisation of entity's goals whilst maintaining a balance between IT value and IT risks (Elazhary et al., 2022). It is important to further note that as IT governance mechanisms are aimed at ensuring the alignment between IT and business objectives, this results in achieving the desired IT aptitude that serves the entity's objectives. Peterson, (2004) concluded that entities with more effective IT governance will most likely result in a more effective and efficient IT capability. Furthermore, IT governance mechanisms enhances effective IT capability which improves an entity's innovations (Zhen et al., 2021).

Different frameworks have been established to assist the board in overseeing IT governance, these includes to mention a few the Control Objectives for Information and related Technology (COBIT 5), COSO, ISO/IEC20000, ISO/IEC 27000, ISO/IEC 27002 and ISO/IEC 38500 (De Haes et al., 2013; Jordaan, 2019). Other regulations and standards have also been developed in different countries which includes King IV code of governance developed in South Africa to which assists listed and non-listed companies JSE with corporate governance guidelines, Sarbanes-Oxley Act (SOX) developed in the USA to guide organisations on governance issues in USA, ISO/IEC 27002 standards which assist with guidance on IT security techniques and risk assessments and risk managements (Ngwenya, 2015). The Commission of Sponsoring Organisations (COSO) provided organisations with comprehensive guidelines on internal controls, risk management and fraud deterrence aimed at improving organisational performance and to reduce IT risk and fraud. Information Technology standards of best practise for information technology management ISO/IEC 27000/2 guidelines have been designed to assist with information security administration and management. Corporate governance on information technology ISO 38500 guidelines have been designed to support organisations to fulfil their regulatory and legal obligations on the use of IT (Gheorghe, 2010). ISO/IEC 20000 standards provides guidelines on the service management which includes IT services (Jordaan, 2019).

COBIT 5 frameworks which is part of IT governance assist organisations in achieving their objectives for the governance and management of IT and helps to create value from IT through maintaining a balance between the benefits and risk levels on IT use (Mangalaraj et al., 2014). According to ISACA, (2012) COBIT 5 is made up of five key principles which allows an organisation to establish an effective and efficient IT governance, these are summarised in figure 2.3 below.

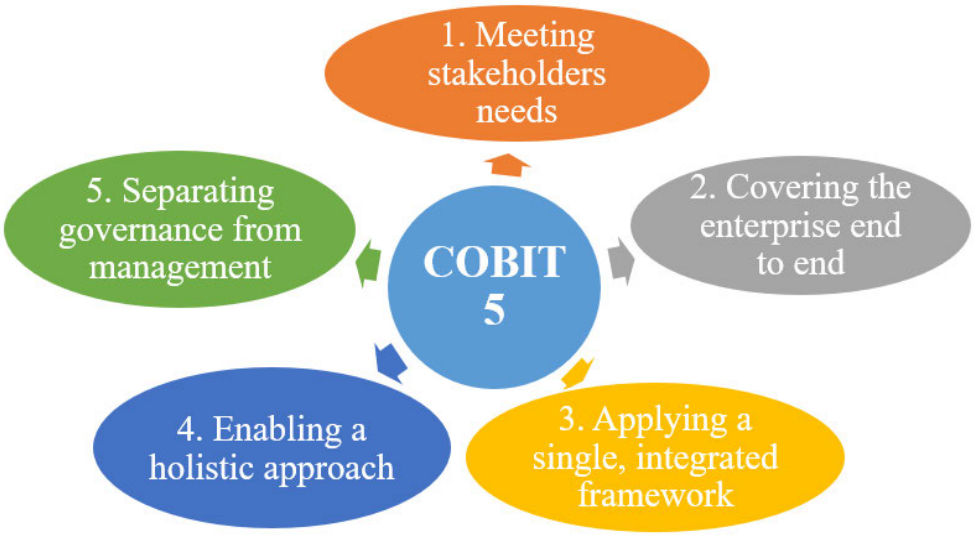


Figure 2.3: COBIT 5 principles

Source: ISACA (2012:8)

COBIT 5 first principle requires an organisation's IT governance to designed in a way which meets the stakeholder needs, this therefore means that the board of directors should consider all the stakeholder and investors needs in establishing IT governance mechanisms. The second principle requires an organisation to cover enterprise IT governance end to end, meaning that the alignment of enterprise and IT applications, integration of IT governance and corporate governance should be seamless. Third principle requires an organisation to apply a single integrated framework in managing IT and IT resources. The fourth principle requires an organisation to enable a holistic collective approach in the governance of IT. The fifth principle requires an organisation to separate governance from management, this enables to board of directors to take the responsibility of IT governance whilst executive management takes the responsibility of managing the entity's IT resources utilisations (ISACA, 2012). COBIT 5 relies on effective corporate governance practises. An organisation's board of directors is expected to set the direction and management is required to implement the plans and monitor the activities to ensure that they align with the direction set by the board of directors with the aim of meeting a company's objectives (Mangalaraj et al., 2014).

2.4.4 Information Technology Risk Management

Risk management is defined as a process of identifying the exposures and threats from the framework of an entity as well setting up policies and procedures in order to minimise the impact on the use of IT resources (Gheorghe, 2010). Muslih et al. (2020) concurred with Gheorghe, (2010) through defining risk management as a set of policies and procedures designed by a company to monitor and control the company's exposure to risks. IT risk management is a component of the overall responsibility for risk management assigned to the board of directors. IT risk management is more focused on the risks exposed to entities as a result of using IT systems and these risks are integrated into the overall risk management framework (Marx & Hohls-du Preez, 2017). Risk management constitutes an integral part of Information Technology Governance and COBIT 5 incorporated the core elements of IT risks in the governance of IT framework (Debreceny, 2013). It is important to note that risks cannot be eliminated, however with risk management the risks are continuously monitored and reduced to an acceptable level which results in creation of sustainable value. Risk management is important to a company, not only because it is an essential component of corporate governance and King IV and the Companies Act, but also because the company strategy should be aligned with business risks including IT risks (Raemaekers & Maroun, 2014).

Risk management allows IT managers and the executive management to balance the business operations, costs and its strategic objectives with the protection of IT application systems and aptitudes of an organisation to achieve its goals (Tohidi, 2011). Risk management is a cornerstone of IT governance as it ensures that the entity's strategic goals are not imperilled by IT failures and malfunctions (Hardy, 2005). ISACA, (2012) defined risk management in relation to IT and information systems as a process designed to identify the threats to its IT systems and vulnerabilities exposed to the organisation's operations due to the use of IT systems (Jordaan, 2019). In addition, an organisation should develop measures and internal controls aimed at arresting or reducing these risks to acceptable levels, it is therefore important to note that risk management is aimed at ensuring integrity, availability and confidentiality of IT systems to an organisation (Jordaan, 2019). Effective risk management enables an organisation to monitor strategic risks and use opportunities related to its business model to achieve its strategic objectives.

According to COSO, (2004) Enterprise risk management (ERM) is a process effected by a company's board of directors and executive management aimed at identifying potential activities which may affect the company's operations as well as to manage and monitor the

risks to enable them to achieve the company's objectives. ERM framework therefore helps companies to achieve their objectives whilst avoiding any shortfalls caused by IT risks. Information technology risk management consist of risk analysis which deals with the gathering of information on risks exposures as well as risk management which deals with the monitoring and control of risks identified during the risk analysis to ensure that these risks are kept at an acceptable level (Hardy, 2005). IT risk management and disclosure is important as it ensures transparency of information provided to all stakeholders (Hohls-du Preez, 2016). King IV code recognises the importance of IT in business operations and the risks associated with it. King IV's principle 11 explicitly requires the board of directors to manage and govern technology and information in a way that helps businesses define key goals and achieve strategic goals (IoD, 2016). It further provided guidelines on IT risk management and what should be disclosed which includes:

- Structures and processes of IT management;
- Key areas of focus for the period;

2.4.5 Information technology governance and risk disclosure literature

Several studies on South African JSE listed entities' compliance with IT governance and risk disclosure requirements as well as risk management and disclosures have been identified in literature. To start with, Janse van Vuuren (2006) investigated disclosure of risk management policies in financial statements and noted that 33 per cent of the companies investigated complied to King II governance and risk disclosure requirements, including IT. Marx et al. (2016) did a study on information technology governance disclosure compliance of JSE-listed companies and found that IT plays an important role in the easing of company operations. Although IT application systems are very vital for organisational success, its rapid change over time has continuously exposed organisations to new risks which should be addressed through effective IT governance (Marx et al., 2016). Marx et al. (2016) submitted that 47 per cent, which represented 19 out of 40 companies, were fully compliant; 15 per cent, which represented 5 companies, were partially compliant, and 38 per cent, which represented 15 companies, did not comply with King III's IT governance and risk management disclosure requirement. The findings of Marx et al. (2016) on IT governance and risk disclosure however reflected a significant improvement from the previous studies completed by van Vuuren (2006), which indicated 33 per cent compliance by listed entities to King II risk governance disclosure requirements.

Ngwenya (2015) analysed the Information Technology Governance disclosure of top 40 JSE listed companies' compliance with King III IT governance requirements in 2015 and a conclusion was drawn that only 40 per cent of the companies fully complied, 25 per cent partially complied and the remaining 35 per cent did not comply with any of the IT governance disclosure requirements. The author argued that the reasons for non-compliance or partial compliance could be because of a company's board of directors and executive management failing to understand or interpret the King III code's disclosure requirements on IT governance and risks. van Vuuren (2020), noted that all the top 40 JSE listed companies investigated disclosed all the 17 principles of King IV in their annual reports, hence effectively complied with King IV principles of good corporate governance. Companies declared and disclosed compliance with King IV principles mainly to adhere to some of the JSE listing requirements, and not as integral to value creation and good governance as envisioned by King IV (van Vuuren, 2020).

Marx and Hohls-du Preez (2017) investigated the IT risk management disclosures in the integrated reports of the top 40 JSE listed companies. They note that the use of IT has brought with it several benefits that increase productivity and efficiency. However, entities using IT applications are exposed to significant risks that could impact their ability to continue as a going concern. The results indicated that out of the 40 listed entities selected, 87 per cent of these disclosed their IT risks with sufficient detail provided to stakeholders and investors, which enables stakeholders to understand the risks entities are exposed to, and 13 per cent of the entities did not disclose their IT risks in the integrated reports, which is disconcerting. In addition, 87 per cent of the companies disclosed a detailed risk management process and procedures. Furthermore, they indicated that IT risks were disclosed as significant risks mainly relating to going concern, and in the event of a disaster and protection of personal information and confidential information (Marx & Hohls-du Preez, 2017). In a similar study by van Vuuren (2016) on 80 JSE listed companies and the results showed that only 12% of these companies fully complied with all King II disclosure requirements on risk management and internal controls. Post the implementation of King III, research shows that when disclosing risks, 90% of the assessed companies disclosed their risks and how these risks were reduced as recommended in King III. Furthermore, Mosiane (2018) investigated the risk management disclosure specifically in the consumer goods sector and revealed that 81 per cent of the companies investigated disclosed the risks recommended in King III principles of good governance.

Schutte and Marx (2018), investigated the role of information technology and risk management on South Africa businesses, focusing on the JSE top 40 listed companies. Like other studies, it was found that more than half of the companies disclose their IT risks and how to effectively mitigate these risks. The author concluded IT governance plays a very critical role in the risk management processes. Owing to a rapidly changing IT environment, a company's board of directors and senior management is expected to clearly understand the critical role that IT plays in risk management processes. Furthermore, Jordaan (2019) investigated IT governance disclosure practices in the integrated reports of JSE-listed companies and revealed that similar to other studies the disclosure of IT governance by these companies was partial or limited.

The literature above constantly reveals that more focus has been put on King II and King III Codes of Corporate Governance, IT governance and risk disclosure; however, there is a gap in literature on companies' compliance with the updated King IV IT governance and risk disclosures. This study sought to fill the gap, as it is aimed at analysing the top 40 JSE listed entities' compliance with the recently adopted King IV principles on IT governance and risk disclosure requirements. The study further analyses the similarities and differences between King IV and other International Standards, which include International Organisations for Standards (ISO 27002, 38500), COBIT 5, Sarbanes-Oxley Act and International Standards of Auditing 315 on IT governance and risk disclosures.

2.4.6 Integrated Reports & Risk Disclosure

The International Accounting Standard sets out the overall requirements for financial statements. Companies are required to prepare general purpose financial statements, and the purpose of this is mainly to satisfy the needs of users who will not be able to request the company to provide the reports (IASB, 2011). In addition to the general-purpose annual financial statements, integrated reporting was introduced with the aim of providing clear disclosures of all the relevant information that is useful to the users. An integrated report is a document in which a company summarises its strategy, performance and activities to its stakeholders in a manner which allows them to assess how the entity creates value in the short, medium and long term (Marx & Mohammadali-Haji, 2014; Roberts et al., 2020). Furthermore, the purpose of integrated reporting is to support integrated thinking, decision-making and actions that drive value creation in the short, medium and long term (Moolman et al., 2016). In

addition, integrated reporting allows for better communication of an entity's strategy as well as advancement of sustainable goals (Cheng et al., 2014; De Villiers et al., 2014). With the use of integrated reporting, stakeholders can assess the entity's ability to create sustainable value (Dumay et al. (2016), as well as combining financial, intellectual, social, and environmental capitals in a common document (Abeysekera, 2013).

Integrated reporting (IR) provides stakeholders with both non-financial and financial information as well as sustainability information in one report which indicates the entity's performance; this is considered a more holistic approach in which a company presents its strategy together with financial and non-financial information (Marx & Hohls-du Preez, 2017; Moolman et al., 2016; Phesa, 2021; Surty et al., 2018). Integrated reporting has the potential to shift the thinking of stakeholders to align the belief of maximisation of profit with the wellbeing of the environment and the society (Adams, 2015). According to James (2014), IR helps stakeholders to understand the interrelationships between an entity's financial performance and its impact on the society, environment, and it enhances decision makers' understanding of various operations, risks, opportunities and functions of the entity in a comprehensive nature. Integrated reporting enhances ethical, reliable and unbiased reporting of an entity's information and impact on society, environment, people as well as profits comprehensively (James, 2014).

Moolman et al. (2016) also noted that integrated reports/corporate governance reporting goes beyond the provision of financial and non-financial information by providing investors and other stakeholders with information relating to the entity's current and prospective risks as well as opportunities. In addition, integrated reporting has been supported by King IV code of corporate governance, which encourages entities to practise good governance and the disclosure of information to stakeholders. Therefore, integrated reporting enables the King IV disclosure requirements, which include IT governance and risk disclosures (Surty et al., 2018). King III, together with the new King IV, advocates for integrated reporting on a voluntary basis, namely King III using "apply or explain" rule-based approach and King IV's "apply and explain" outcome-based approach (Dumay et al., 2016; IoD, 2016). King IV requires an integrated report to provide stakeholders with insights into how value has been created and can be created in the future (Marx & Hohls-du Preez, 2017). This can therefore be achieved by managing the current risks that have the potential to affect future value realisation. Besides King IV, the disclosure of corporate governance has become a mandatory requirement of the Johannesburg Stock Exchange to maintain a company listing, thus making it essential for listed

companies to prepare integrated reports and disclose their corporate governance practises including how IT risk governance is achieved (Jordaan, 2019).

Integrated reporting enables risk disclosure which is important to stakeholders and investors as it enables them to have knowledge of the risks affecting an entity and entity's risk management practises as well as to assess the risk tolerance levels before investing in an entity (Viljoen et al., 2016). Risk disclosure is very important; however, researchers have also noted that management is not keen on providing adequate risk disclosure due to the fear of negative effects that this disclosure may have on the company (Hohls-du Preez, 2016). Management is concerned about the costs an organisation may incur from its competitors because of disclosing all the risks but disclosing risks can increase the transparency and reliability of the annual report. Management discloses the company's risk exposures as well as plans and strategies to mitigate these risks in the integrated reports (Madrigal et al., 2015). Risk disclosure plays an important role as it protects the interest of investors and stakeholders, which results in good governance (Madrigal et al., 2015). A complete disclosure of risks in the integrated report provides investors and stakeholders with all the information pertaining to risks, which may be used to assess a company before making an investment decision. Disclosure of clear, understandable and readable information in the integrated reports will attract potential investors, particularly the small investors (Hohls-du Preez, 2016). Risk disclosures also reduce stakeholders and potential investors' uncertainties on the future cashflows and continuity of an organisation. Furthermore, risk disclosure helps to ensure transparency and reliability of the integrated reports as investors and other stakeholders are provided with all the information including risks for them to assess and analyse before making investment decisions (Marx & Hohls-du Preez, 2017).

2.4.7 King IV IT governance and risk disclosures

King IV code defined corporate governance as an ethical and effective leadership of board of directors on establishing a good principled culture, excellent performance, legitimacy and efficient control of an organisation (IoD, 2016). The code of corporate governance was introduced to accommodate and provide guidance on changes in the Companies Act 2008 and changes in the governance structure and it came into effective on 1 April 2017 (IoD, 2016). The Johannesburg Stock Exchange (JSE) has included in its mandatory listing requirements that all companies listed should comply with the principles and recommendations of good corporate governance as per King IV (JSE, 2017b). King IV included information technology governance as part of an entity's corporate governance requirements and further places greater

prominence on the important IT governance, IT security governance and governance of IT risks (Jordaan, 2019). It recognises the significance of using information technology application systems by companies and the risks associated with it.

The principle 12 of King IV requires the board of directors to manage and govern company's information technology in a way which helps a company to achieve its strategic objectives (IoD, 2016). King IV recommended clearly that the board of directors should take the full responsibility on the governance of information technology through setting the path on how information technology and its risks should be addressed in a company to achieve its strategic and operational objectives. In addition, the board is required to oversee the integration of information technology risks into the company's risk management as well as to identify and respond to risks, including cyber-attacks (IoD, 2016). The King IV code also requires organisations to provide sufficient disclosures which enables its stakeholders to assess and evaluate the quality of entity's governance structure (IoD, 2016). King IV further recommends disclosure in relation to information technology which includes:

- Disclosure on the overview of the plan for governing and managing information technology,
- The identified key areas of focus for the year, objectives, changes in IT policies and procedures, significant acquisitions, major IT incidents and remedial actions,
- The board and management actions undertaken to manage and monitor the effectiveness of information technology and how the outcomes have been addressed in ensuring that IT enables the company to achieve its strategic objectives.
- Areas of future focus (IoD, 2016).

Furthermore, principle 11 of King IV requires the board of directors to manage and govern company's risks in a manner which helps a company to achieve its objectives (IoD, 2016). It recommended clearly that the board of directors to undertake the duty on risk governance through providing a clear direction on how these risks will be addressed and reduced to acceptable levels. It encompasses that in order for a company to achieve its objectives management should consider potential benefits and drawbacks of each prospective IT opportunity and the risks which can be exposed to the company as a result of undertaking these IT opportunities (IoD, 2016). King IV further recommends disclosure in relation to risks which includes:

- Disclosure on the overview of the arrangements for governing and managing risks,
- The identified key risks and IT risks that the company faces, including undue, unexpected or unusual risks and risks taken outside risk tolerance levels,
- Disclosure of the nature and extent of the risks as well as opportunities without compromising company sensitive information,
- The board and management actions undertaken to monitor the effectiveness of risk management and how the outcomes have been addressed to ensure risk management enables the company to achieve its strategic objectives (IoD, 2016).

2.4.8 ISO/IEC IT governance and risk disclosures

The International Organisation for Standardisation and International Electrotechnical Commission 38500 as well as other ISO's 27000, 27001, 27002 provides a framework for effective governance of IT, risks and security, which is aimed at assisting the board of directors and executive management to understand and fulfil their obligations in respect of a company's use of IT application systems (Standardization, 2008). ISO 27001 defines IT governance as a framework developed for leadership, organisational structures and business process standards and compliance to ensure that a company's IT application systems support and enable the achievement of its strategic objectives. The main goals of IT governance are to ensure that IT application systems are utilised to add value to the company as well as to mitigate the risks that are associated with the use of IT (Mohamad & Toomey, 2016). In addition IT governance seeks to promote effective use of IT application systems and to ensure that IT systems meets the company objectives which includes among others, IT systems alignment with business, effective use of IT systems by the business to maximise its benefits, using IT systems responsibly and appropriately managing risks exposed due to the use of IT resources (Mohamad & Toomey, 2016).

ISO/IEC 38500 provided six principles which were designed to guide the directors and executive managing in doing their duties with regards to evaluating, directing, and monitoring the use of IT systems in order to establish effective governance of IT and information systems in an organisation and these includes, (i) responsibility which involves allocating responsibilities relating to the use, effective management of IT systems and monitoring IT governance mechanisms, (ii) strategy which involves evaluation of developments of IT applications systems and business processes ensuring that developed IT systems assist the

company to achieve its strategic objectives, (iii) acquisition which involves evaluation of IT application systems which will be suitable for use and which can easily be aligned with the business operations and assessing risks which a company can be exposed to and the benefits driven from the IT systems before any purchase of IT application systems, (iv) performance which involves assessing how IT application systems used in a company supports its processes to achieve its strategic objectives, (v) conformance which involves regular evaluations of IT systems to ensure that it meets the organisation's standard set as well as fulfilling the compliance standards, (vi) human behaviour which involves assessing how employees effectively use the IT application systems as well as systems maintenance aimed at achieving the company's strategic objectives (Jordaan, 2019; Rama & Gunawan, 2020). To ensure effective IT and risk governance ISO 38500 further recommended organisational practises which includes the following:

- The board of directors and executive management should design policies and procedures to guide IT projects and IT application systems,
- The board of directors and executive management should monitor and evaluate IT improvements and new IT projects, new IT application systems acquired or developed,
- The board of directors and executive management should constantly assess the performance on IT projects and IT application systems,
- The board of directors and executive management should align the company strategic objective with the IT application systems (Ahuja & Chan, 2015).

There are five main areas in IT governance critical to the improvement of an entity's value and processes which includes, strategic alignment, risk management, value creation, resources management and performance management (Rama & Gunawan, 2020). Strategic alignment focuses on IT systems alignment with the company strategy, objectives and risks exposed to a company because of using IT systems, value creation focuses on the execution of the entity's strategy ensuring that IT application systems used will enable the entity to achieve its strategy and objectives. In addition resource management ensures that IT resources which includes IT application systems, infrastructure and skilled staff are available and lastly performance management focuses on monitoring and assessing the implementation of the entity strategy with the use of IT systems to ensure the entity achieves its objectives and deliver its services (Rama & Gunawan, 2020).

To ensure confidentiality and protection of information international standards ISO 27000, 27001 and 27002 were designed to provide guidelines on how organisations can achieve IT security, protect privacy data, prevents data and cyber security breaches, fraudulent accounting systems and attacks on IT applications systems (Disterer, 2013). These ISO standards offer organisations an opportunity to align their IT systems policies and procedures with a suitable level of information security which enables protection of its information. It is further important to note that ISOs are not enforceable but however provides voluntary IT governance disclosures which can be used by organisations to ensure effective IT governance and disclosure in a clear and understandable manner by stakeholders (Ngwenya, 2015).

2.4.9 Sarbanes-Oxley Act (SOX) IT governance and risk disclosures

The SOX Act was enacted in the United States with the aim of protecting shareholders and other stakeholders from financial reporting errors and fraudulent activities by companies as well as to improve corporate reporting and disclosure practices (Ngwenya, 2015). The Act requires organisations to disclose information relating to IT governance and its mechanisms for internal controls. The Act defined corporate governance as an ethical behaviour by those charged with governance in the generation and presentation of company value to the shareholders (Kim et al., 2008). IT governance is a subset of corporate governance that focuses on the performance of information technology systems and risk management. It is important to note that after the enaction of the SOX Act there has been a rising interest on IT governance for publicly trading companies (Brown & Nasuti, 2005b). The key sections of SOX compliance which directly involves IT governance and IT controls includes section 302 and 404 (Brown & Nasuti, 2005b; Kim et al., 2008). Th Sarbanes Oxley Act consist of several sections that companies should comply with, but only two of the most important sections relates to IT governance and controls (Ngwenya, 2015).

Section 302 of SOX applies to company financial statements, related financial information. It requires management to provide disclosure of the company's internal controls, data safeguard procedures, assurance from fraudulent transaction reporting thus ensuring that financial reports provided to stakeholders are free from errors, faults, interference and inaccuracies (Brown & Nasuti, 2005a; Kim et al., 2008; Ngwenya, 2015). It also requires a disclosure of deficiencies in the company's internal controls and fraud regardless of the deficiencies being material or immaterial (Hall & Liedtka, 2007). A company's internal controls relates to policies,

procedures and practises aimed at reducing its exposure to risks thus helping the company to achieve its business objectives (Kim et al., 2008). Section 302 of SOX holds the company chief executive officer (CEO) and the board of directors accountable for good governance together with accuracy of financial reporting as well as the chief information officers (CIO) for IT governance risk management and business continuity (Brown & Nasuti, 2005a; Stults, 2004). Section 302 of SOX requires the CIO to certify acknowledging the undertaking of responsibility on the establishment and maintenance of an organisation's internal controls as well as the evaluation of the efficacy of the systems internal controls to avoid or reduce risks exposure to the company (Act, 2002). It is important to note that the disclosure and certification of internal controls required by Section 302 are not detailed in the Act, however these internal controls include controls on the company's use IT application systems in its operations which therefore forms part of IT governance.

According to section 404 those responsible for governance are required to conduct an annual review of the effectiveness of internal controls and report to the Securities and Exchange Commission (SEC) (Brown & Nasuti, 2005a). The report is required to include a clear detail on the management responsibility for the establishment and maintenance of internal control structure including IT controls and financial reporting procedures (Ngwenya, 2015). Adoption of SOX resulted in an increased focus on business IT processes and controls as IT applications systems which supports financial processing and therefore should be assessed to ensure its effectiveness under Section 404 (Dhillon & Mishra, 2006). To ensure compliance with SOX, companies are required to constantly improve information quality and increased IT innovations which enhances cost-efficient and real time financial reporting (Kim et al., 2008).

To ensure effective assessment of the internal controls and IT application controls different control assessment frameworks which includes, Committee of Sponsoring Organisations (COSO) and Enterprise Risk Management (ERM) have been designed aimed at managing and reducing risks (Brown & Nasuti, 2005b). The COSO framework has divided IT internal controls into two categories, namely the general IT controls and the IT application controls. General IT controls include but not limited to, information centre operations, application software control, access control, application systems development and maintenance controls whereas application controls includes controls on information processing and integrity of transactions, authorisations and validity (Brown & Nasuti, 2005b). Furthermore, it is important to note that an assessment of internal controls cannot be completed without assessing controls

around information security mainly because an insecure system is not considered as a reliable source of financial reports due to possible access by unauthorised users which can result in processing of unauthorised transactions or manipulation of financial reports (Stults, 2004). Stults (2004) further noted that application and assessment internal controls is deemed incomplete if these do not address IT and risks governance when reporting and disclosing a company's financial performance.

2.4.10 International Standards on Auditing 315 IT governance and risk disclosures

The use of IT application systems contributed significantly towards effective communication, accuracy, creativity and innovation by companies. IT application systems further facilitates services, improves productivity and integrates hardware and software as well as infrastructure (Al-Rahamneh, 2016). Information system management involves the basic configuration of integrated systems, software, equipment and human resources to ensure the collection and processing of information as well as providing stakeholders with the accurate information on the right time with lower cost and high quality internal environment (Al-Rahamneh, 2016). Companies have adopted the use of IT to analyse problems and facilitate decision making and communication with its stakeholders. The computerisation of IT systems has an impact on an organisation's internal controls mainly through the ISA 315 standard (Wei-hua, 2011). The ISA 315 standard aims to identify and assess risks exposed to a company by understanding the company and its environment. The process involves an assessment of the entity's IT application systems and risks to ensure that its IT application systems are effectively utilised to support the entity to achieve its strategic goals as well as minimising the risk exposure (Al-Rahamneh, 2016). Auditors are required to perform assessments to understand the entity, environment, and internal controls, including IT controls, allowing the auditor to determine whether there any inconsistencies between the company's IT strategy and its strategic goals, as well as any changes to its IT systems and internal control environment which are significant for the financial period (Ngwenya, 2015).

2.5 Gaps in literature

The literature has constantly revealed that quite a significant focus has been placed on King II and King III Codes of Corporate Governance, IT governance and risk disclosure over the years. Many researchers have assessed company's disclosure compliance when King II code of corporate governance was introduced as well as after the introduction of King III code of

corporate governance mainly in the field of IT governance and risk disclosures. As much as there are a lot of studies completed in the field of corporate governance mainly in assessing disclosure compliance on King codes corporate governance specifically IT and risk governance, there are still gaps identified in the literature as there is very limited studies which focused on company's disclosure compliance with the recently published King IV IT governance and risk disclosure. This study seeks to fill the identified literature gap as it is aimed at analysing the top 40 JSE listed entities' compliance with the recently adopted King IV principles on IT governance and risks management disclosure requirements. The study is important as it assists regulatory bodies, standard setters, and other institutions of corporate governance.

2.6 Chapter Summary

Literature shows rich insights from theoretical and empirical studies in literature from stakeholder, stakeholder theory, JSE top 40 listed companies, integrated reports, information technology, risk governance, risk management and King IV IT governance and risk disclosure compliance as the overarching phenomena. Literature also revealed that 100% score was not achieved on the King II and III compliance on IT governance and risk disclosure and therefore making it important to analyse the compliance on the recently published King IV requirements on IT governance and risk disclosure. Literature further noted the importance and role played by information technology to support organisations to achieve they strategic goals as well as the risks introduced by the use IT application systems. The chapter also identified COBIT 5 IT governance frameworks established to help companies realise their goals on governance and management of IT applications aimed at creating value and sustaining a balance between the benefits and risk levels on IT. ISO 38500 provided six main principles designed to provide guidance to the board of directors in doing their duties to ensure effective IT governance and risk management. The disclosure of IT governance and risk management practices and corporate governance in the financial statements should be of such high quality, that stakeholders should have no doubt that an appropriate balance between risks and rewards exists in the company.

The next chapter presents research methods applied, including data collection methods, sampling, and analytical tools.

CHAPTER 3 RESEARCH METHODOLOGY & RESEARCH DESIGN

3.1 Introduction

Bell et al. (2018) define the term research methodology as a data collection method, which outlines a roadmap of how the researcher will explore and gather. Research is also defined as a series of analysing, reviewing or assessing the study aimed at reaching a new conclusion (Maree & Van der Westhuizen, 2009). This chapter explores the research methodology followed in this study including research philosophy, approach, strategy, design, population, and data validity. The honeycomb model of research method was used to explain the components of the research methodology applied by the researcher in this study.

3.2 The Honeycomb model of Research Methodology

Wilson (2014a) introduced the honeycomb of research model framework aimed at differentiating research methodology from research design. In other words, research design is a framework used to collect and analyse data whilst research methodology refers to the means or methods of data collection (Wilson, 2014b). The honeycomb model of research methodology consists of six main elements, namely (i) research philosophy, (ii) research approach, (iii) research strategy, (iv) research design, (v) data collection, and (vi) data analysis (Wilson, 2014a). These are shown in figure 3.1 below.

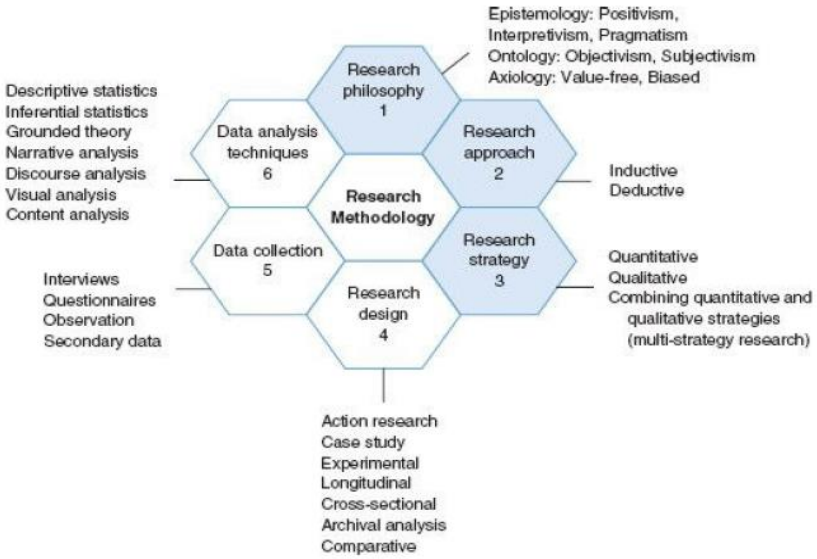


Figure 3.1: The Honeycomb model of Research Methodology

Source: Wilson (2014:32)

3.2.1 Research philosophy

A philosophy is considered as a study of important nature of knowledge, reality and existence used mainly in the field of study. Research philosophy is regarded as a researcher's view or thinking on information gathered, which may influence the approach they use to conduct the research studies (Wilson, 2014b). According to Bell et al. (2018), there are two different beliefs, namely objectivism and subjectivism. Objectivism holds that there is a measurable reality whilst subjectivism considers reality to be relative (Bell et al., 2018; Hudson & Ozanne, 1988). Positivism considers an objective view when conducting a research study; a positivist approach detaches the researcher from the subjects of the study and it hence carries the study in a scientific and objective nature (Wilson, 2014b). With positivism/objectivism, the researcher's own ideas, feelings and biases have no part in the study, and will therefore not influence the results of the study. Subjectivism can be connected to interpretivism as it involves the examination of motivations and social interactions of respondents by the researcher (Wilson, 2014a).

The study used an interpretivist philosophy to analyse the IT governance and risk disclosures by the JSE top 40 listed entities to ensure compliance with the disclosure requirements set forth by King IV. A qualitative approach through content analysis was applied to the analysis of the annual reports of the listed entities selected. Companies are socially formed, and it is therefore expected that they will apply subjective meanings to what constitutes IT governance and risk management disclosure and the King IV disclosure requirements. Likewise, they also use subjective meaning on the nature of what should be disclosed relating to IT governance and risk management as well as the extent of disclosure. This is in conjunction with the epistemology that recognises that each company is different and therefore each company's IT governance and risk disclosures are expected to be different. The extent of IT governance and risk disclosure in each company's integrated reports was analysed and interpreted based on the King IV requirements and recommended practices.

3.2.2 Research approach

Bryman (2003) identifies three approaches of reasoning, namely inductive, deductive, and abductive reasoning approaches. Moving from the specific to the general, induction while beginnings with the general and ending with the specific is known as deduction and generalising the interactions between specific and general is known as abduction (Bell et al.,

2018; Bryman, 2003). Examples of the deductive approach of reasoning includes arguments based on laws and regulations whilst inductive approach of reasoning examples include arguments based on experience. Inductive research approach is conducted mainly using the views of the targeted group to generate a theory, whilst with a deductive research approach the researcher starts with theories and then hypothesis to support or oppose theory (Bryman, 2003). Deductive research approach is often linked to quantitative research methods, whilst inductive research approach is associated with qualitative research methods (Bell et al., 2018).

A deductive research approach can be defined as a development of a hypothesis which is based on an existing theory and it uses the theory to develop a strategy (Wilson, 2014b). In this study the existing theory is the King IV principles, which forms part of the corporate governance framework. King IV principles and recommended practices were used by the researcher to develop a disclosure checklist and measure it against the IT governance and risks disclosed in the annual and sustainable reports to analyse the extent of a company's acquiescence with King IV requirements. In order to analyse the IT governance and risk disclosures in the annual and sustainable reports of the top 40 JSE-listed firms, a deductive research approach was used.

3.2.3 Research strategy

Research strategy involves an examination or investigation with the intention of identifying and interpreting facts on recognised philosophies/ principles (Bhat et al., 2020). Researchers use different types of methods to conduct research, and these include qualitative, quantitative, and mixed methods.

Quantitative research method: It is a method of collecting information and examining it with the main aim of drawing conclusions (Bell et al., 2018). This method uses statistical tools to examine and analyse the information collected.

Qualitative research method: It is a method which mainly uses enquiries and uses other studies and research papers which have been completed before by other authors and researchers as well as interviews of subjects under the study. Qualitative research methods do not use statistical tools in reviewing information (Bell et al., 2018). The quantitative research method is also referred to as a positivist approach of analysing information whereas the qualitative research method is often referred to as an anti-positivist research approach (Bellamy, 2011).

Mixed research method: It relates to the research method which makes use of both positivist and anti-positivist approach to reviewing and analysing data to answer the problem in question (Bell et al., 2018; Clark & Creswell, 2008).

This study applied the qualitative research approach as it sought to conclude on the extent of the JSE top 40 listed firms' IT governance and risk disclosure compliance to King IV recommended practices. Furthermore, the qualitative approach, through content analysis, was conducted to identify similarities and differences between King IV, COBIT 5, International Organisations for Standards (ISO 27002, 38500), Sarbanes-Oxley Act, and International Standards of Auditing 315 on IT governance and risk disclosure requirements and likely recommendations on IT governance and risk disclosure that have potential to enhance King IV provisions. The research strategy is consistent with prior studies conducted in the field of IT governance and risk disclosure (Jordaan, 2019; Ngwenya, 2015; Sityata, 2020; Sityata et al., 2021).

3.2.4 Research Design

The term "research design" refers to a precise framework or strategy that assists in guiding the research through the research process, which increases the possibility of attaining research objectives (Wilson, 2014). It is useful as it assists the researcher to design the overall research study in an appropriate manner with the aim to obtain relevant data to address the research problem and answer the research questions (Leedy et al., 2014). Research designs vary from investigational, cross-sectional or social survey, longitudinal and archival research (Bell et al., 2022; Saunders et al., 2009). The case study/Ex post facto/archival research design used in this study is defined as a design which relates to events which have occurred or conditions which are already in existence (Bell et al., 2022; Ngwenya, 2015). The study was conducted using the case study/Ex post facto/archival design mainly because the King IV principles and recommended practices on IT governance and risks already exist and the annual integrated reports which were used have been published by the companies for public use.

A detailed analysis of literature on corporate governance and King IV was used to identify the key IT and risk disclosure requirements and to design a disclosure checklist (Mosiane, 2018; Raemaekers & Maroun, 2014). The disclosure checklist was used to drive the assessment of the level of IT and risk governance disclosure by JSE top 40 listed entities in their integrated reports and corporate governance reports. To achieve the study's primary and secondary objectives, a qualitative content analysis was followed to assess the degree to which JSE top

40 listed entities conform with King IV's IT governance and risk management disclosure. In addition, a review was conducted to identify similarities and differences between King IV and other International standards ISO 27002, 38500, COBIT 5, SOX and ISA 315 on IT governance and risk disclosure requirements and the likely recommendations aimed at enhancing King IV provisions.

3.2.5 Data Types and Sources

Data types and sources include a process of obtaining and recording information in a manner which will assist a researcher to analyse data (Salkind & Van Zyl, 2014). Secondary data was used by the researcher as the data was already available in the integrated/annual reports, sustainability reports, and corporate governance reports found on entities' websites. The 2021 integrated, sustainability and corporate governance reports of the top 40 listed entities were extracted and analysed to confirm the IT governance and risks disclosed to ensure compliance with the King IV and international standards. Content analysis was used by the researcher to identify similarities and differences between King IV and international standards, which includes ISO 38500, 27000, 27001, 27002, ISA 315, SOX requirements on IT governance and risk disclosure requirements and the likely recommendations aimed at enhancing King IV provisions.

3.2.6 Data Collection Methods and Research Instruments

Secondary data in the form integrated/annual reports as well as King IV and international standards were collected and analysed through qualitative content analysis. An IT risk governance and management disclosure checklist was designed and used in this study. The checklist was used mainly because it is cheap and allows the researcher to perform a qualitative study without the need for an expensive tool. An IT governance and risk management disclosure checklist permits the researcher to assess the adequacy, completeness, and compliance of disclosures with King IV disclosure requirements and other international standards.

3.2.6.1 Disclosure Checklist

A disclosure checklist was used to explore the extent to which King IV principles and recommended IT and risk governance and management practices were applied and explained as well as disclosed in the integrated reports. It also checked compliance. The disclosure checklist was designed based on King IV principle 11, 12 and the recommended practices for effective IT and risk governance and management to determine whether each company applied

a full disclosure, non-disclosure or it obscurely disclosed. The disclosure checklist was divided into two testing stages:

(a) **Stage 1** of the IT and risk governance disclosure checklist consisting of "Yes", "No" and "Obscurely" was used to explore the extent of disclosure through assessing whether each company's IT, risk governance and management disclosures as per King IV had been fully disclosed, or not disclosed or obscurely disclosed in the integrated reports.

(b) **Stage 2** – Whilst stage 1 was intended to assess the degree of IT governance and risk management disclosures, stage 2 was simultaneously used to assess whether IT, risk governance and management practices had been applied. It used "Yes", "No" and, for not fully applied/ partially applied, "Partial" as per King IV.

The process of selecting King IV code principles and recommended practices in developing the disclosure checklist was backed by the following reasons:

- The code acts as one of the governance frameworks designed in South Africa which recommended the best practices for companies to adopt to ensure good corporate governance.
- King IV provided information technology governance through principle 12 and risk governance and management practices through principle 11, and these were recommended for companies to apply in order to ensure good IT governance and effective risk management and governance.
- King IV provided a significant change in the approach through its concept of "Apply and Explain" in comparison with the previous King III's concept of "Apply or Explain". This clearly indicates that companies should explain how they applied the principles and recommended practices. Companies explain their application of the principles and recommended practices through disclosure in different reports, which include sustainability reports, corporate governance reports, economic social, governance reports and integrated reports which are published for the public.

Table 3.1: - IT & Risk Governance Disclosure Checklist designed as the measuring instrument

			STAGE 1 Test			STAGE 2 Test		
			DISCLOSURES			King IV APPLICATION		
No	Category	King IV Recommended Practices (IODSA, 2016)	Yes	No	Obscurely	Yes	No	Partial
1	IT Governance	The board of directors should be responsible for the governance of IT by setting the direction on how IT should be addressed in a company.						
2	IT Governance	The board of directors should approve policy which articulates and gives effect to the set direction on the employment of IT.						
3	IT Governance	The board of directors should delegate to management the responsibility to implement and executive an IT governance framework.						
4	IT Governance	The board of directors should ensure that IT is aligned with the performance and sustainability objcetives of the company.						
5	IT Governance	The board of directors should exercise an ongoing oversight of IT management to ensure alignment and integration of IT risks into organisation-wide risk management.						
6	IT Governance	The board of directors should exercise an ongoing oversight of IT management to ensure proactive monitoring of intelligence to identify and respond to incidents including cyber attack risks and adverse social media risks.						
7	IT Governance	The board of directors should exercise an ongoing oversight of IT management to ensure management of the performance of, and the risks pertaining to, third-party outsourced services.						
8	IT Governance	The board of directors should monitor and evalute significant IT investments and expenditure.						
9	IT Governance	The board of directors should exercise an ongoing oversight of IT management to ensure ethical and responsible use of IT and compliance with relevant laws and standards.						
10	IT Governance	The board of directors should exercise an ongoing oversight of the management of IT to ensure that IT systems supports confidentiality, integrity and availability of information.						
11	IT Governance	The board of directors should exercise an ongoing oversight of the management of IT to ensure protection of privacy of personal information, security of information and protection of IT assets.						
12	IT Governance	The board of directors should ensure dislosure of an overview of its governance and management of IT.						
13	IT Governance	The board of directors should ensure dislosure of key areas including objectives, significant changes in policy, risks including major incidents and significant risks exposed due to IT application systems.						
14	IT Governance	The board of directors should ensure dislosure of actions taken to monitor the effectiveness of IT management and governance and how the outcomes were addressed.						
15	Risk Governance & Management	The board of directors should assume the responsibility to govern risk or through a dedicated committee by setting direction for how risks should be approached and addressed in the organisation including the following; the potential positive and negative effects of the risks in achievement of objectives.						
16	Risk Governance & Management	The board of directors should treat risks as an integral to the way it makes decisions and execute its duties as well as to approve policies which articulates and gives effect to its set direction on risks.						
17	Risk Governance & Management	The board of directors should delegate to management the responsibility to implement and execute effective risk management and governance.						
18	Risk Governance & Management	The board of directors should evaluate and agree on the nature and extent of the risks that an organisations is willing to take in pursuit of its strategic objectives which includes limiting potential loss to the organisation due to IT risks and approving the organisation's risk appetite.						
19	Risk Governance & Management	The board of directors should consider allocating the oversight role of risk governance to a dedicated committee which is the audit committee.						
20	Risk Governance & Management	The board of directors should exercise ongoing oversight of risk management to ensure the following: i. Assessment of risks ii. Assessment of opportunities presented by risks iii. The integration and embedding of risk management in the business activities and culture of the organisation.						
21	Risk Governance & Management	The board of directors should ensure the disclosure of nature and extend of the risks and an overview of the arrangements for governance and managing risk.						
22	Risk Governance & Management	The board of directors should ensure the disclosure of the key risks that the organisation faces, as wll ass undue, unexpected or unusual risks as well as the actions taken to monitor the effectiveness of risk management and how the outcomes were addressed.						

3.2.7 Data Presentation and Analysis Approach

3.2.7.1 Content Analysis

A scientific examination of content with reference to the meaning, context and intent contained in message is characterised as content analysis (Prasad, 2008). Content analysis is referred to as a comprehensive assessment of a particular body of material aimed at identifying and categorising the underlying material into a pattern or theme which can be used to develop a deeper understanding of relevant information through analysis of the contents (Leedy et al., 2014; Raemaekers & Maroun, 2014). Content analysis can be conducted quantitatively through focusing on counting and measuring of the appearance of words in a specific manner or qualitatively through focusing on understanding and discernment of a phenomenon that is already known. Researchers have used content analysis to cross-examine narratives by means of extracting and analysing data and it is the most suitable research method in analysing corporate reports and measuring corporate disclosures (Sityata, 2020).

For the purposes of this study, a qualitative approach was adopted to analyse the annual reports and assess the extent of IT and risk governance disclosures using a deductive reasoning approach, as the principle disclosure requirements and recommended practices already exist and are categorised using the checklist developed. Furthermore, a qualitative content analysis allowed the researcher to comprehend whether the disclosure practices were made or not and also understand whether the recommended IT risk governance and management disclosure practices had been applied or not. A qualitative content analysis was performed on the annual and sustainability reports of the JSE top 40 listed entities, as the integrated/annual report discloses the IT governance and risk management practices which were applied. An IT governance and risk management disclosure checklist was developed based on the empirical study on King IV relating to IT risk governance and management disclosure practices and was designed to extract the content from the integrated reports in order to answer the research questions.

3.2.7.2 Data Analysis and Results

Data analysis and results were done based on the disclosure checklist test for each company selected. An analysis was done on how the JSE top 40 entities are complying with King IV's requirements on information technology and risk governance disclosures as well as the application of King IV principles and recommended practices. To ensure that results are adaptable, an analysis was completed on excel and the records were stored. A content analysis was conducted, and the following approach explained below was the used:

Step 1: Reading the annual/integrated reports highlighting relevant IT risk governance and management disclosures.

Step 2: Reading the annual reports and responding to the disclosure checklist governance principles and recommendations.

Step 3: Evaluating completeness and accuracy of data analysed, results, insights and reported the results in aggregate. The study also compared the results of the previous studies undertaken on King III for improvements on disclosure compliance.

Furthermore, the results on the analysis of similarities and differences between King IV, COBIT 5, International Organisations for Standards (ISO 27002, 38500), Sarbanes-Oxley Act, and International Standards of Auditing 315 on IT governance and risks disclosure requirements were used to draw a conclusion on whether the King IV provisions need to be enhanced or not.

3.3 Research Population

A population is a collection of data/participants from which a simplified sample can be drawn by the researcher to obtain results and make conclusions in a study (Salkind & Van Zyl, 2014). An analysis and review of the top 40 companies listed on the JSE was carried out. The JSE top 40 listed companies are one of the key drivers of South African capital markets and holds a majority stake of 80% on the total JSE entity's value based on market value. The top 40 listed JSE entities represent the largest listed entities in South Africa and are ranked largest by market capitalisation. JSE's top 40 listed companies are considered as having adopted King IV IT governance and risk management as best practices of good governance. All listed entities are required to adhere to the King IV code of corporate governance as part of the listing requirements (Jordaan, 2019).

3.3.1 Top 40 JSE Listed Entities

The top 40 entities listed on the JSE are considered the best performers and key drivers of the South African capital markets (Mamaro & Tjano, 2019). The FTSE/JSE top 40 index represents the 40 largest entities in the South African FTSE/JSE all share index based on full market capitalisation (Pholohane et al., 2020; Russell, 2010). Furthermore, the top 40 JSE index captures more than 80% of the total market capitalisation of all the company shares listed, and they are thus of great public interest and they are also regularly discussed on the public financial platforms (Kotze, 2017; van Zijl & Hewlett, 2022). The top 40 listed companies list in the

FTSE/JSE index changes from year to year depending on the market performances of the listed entities (Barr et al., 2007).

Statistically, it is evident that the top 40 listed entities included in this study represent the largest entities in terms of market value on the stock exchange, and as such, would represent a wide range of stakeholders' interest in South Africa (Marx & Voogt, 2010). Using the JSE top 40 listed entities is consistent with other recent South African-focused studies (Mamaro & Tjano, 2019; Moloi et al., 2021; Pholohane et al., 2020; van Zijl & Hewlett, 2022; Willows & van der Linde, 2016). Organisations listed on the FTSE/JSE are required to publish integrated reports, corporate governance reports and sustainability reports. These reports should include audit committee reports and risk and governance reports. Therefore, the researcher used these reports in this study to analyse the extent to which the entities comply with King IV requirements for IT governance and risk disclosure.

3.4 Research Sample

A sample is referred to as simplified data/participants from the population (Salkind & Van Zyl, 2014). The population used in this study was based on a predetermined "non-probability" sample called quota sampling (Bell et al., 2018). A quota sample of the JSE top 40 listed entities was selected and used in the analysis. JSE top 40 listed entities represents the majority stake of 80% on the total JSE entity's value and therefore very significant for the study. The top 40 listed companies represent different industries in South Africa. The selection of top 40 listed JSE entities is consistent with previous research studies on top 40 listed entities (Hohls-du Preez, 2016; Marx & Hohls-du Preez, 2017; Marx & Mohammadali-Haji, 2014; Ngwenya, 2015; Pholohane et al., 2020; van Zijl & Hewlett, 2022; Viljoen et al., 2016). Accordingly, the sample of top 40 listed JSE entities is deemed most appropriate for this study. The top 40 listed JSE entities' 2020 and 2021 annual/integrated reports were extracted from the company websites in the period 22 – 31 August 2022 after obtaining the ethical clearance which was issued on 19 August 2022.

3.5 Data Validity and Reliability

Validity denotes to whether the research concept actually measures what the researcher has intended to measure (Jordaan, 2019; Saunders et al., 2009). Saunders et al. (2009) define reliability as the ability of the concept to deliver consistent findings. For data to be considered reliable, a similar test undertaken on the same data should provide similar results (Saunders et al., 2009). The data used by the researcher in this study is considered valid and reliable mainly

because the annual/integrated reports are published on company websites and are thus regarded as secondary information available publicly. Integrated/annual, sustainability and corporate governance reports of companies were downloaded from company websites. The data extracted by the researcher are considered valid and reliable as they have been prepared by the companies and published for use by the stakeholders, investors, shareholders, and the public.

Organisations communicate with stakeholders through annual/integrated reports. As part of corporate governance disclosures, King IV has recommended all listed companies to publish their annual/integrated reports for stakeholders and the public to use. It is therefore important for the annual/integrated reports to include adequate and useful information relating to a company's operations, including risks and risk governance practices. The integrated/annual reports provide information to stakeholders which is understandable, relevant, reliable, and comparable, which therefore makes the data used in this study valid and reliable.

3.6 Ethical Considerations

The researcher was granted an ethical clearance before the data collection. Even though the study employed secondary data, ethical clearance was obtained to ensure that the study is carried out in a responsible and ethical manner. Furthermore, ethical clearance was obtained to ensure that there is no harm to the data collected.

3.6 Chapter Summary

The chapter provided the research tools used to collect data required to address the objectives of the study. The chapter outlined the research methodology, which included research approach, research strategy, research designs employed, discussed research instruments used by the researcher and data analysis process. Ethical consideration of the study was also discussed in this chapter. The next chapter provides the presentation, analysis and discussion of the results of the content analysis conducted on the disclosure of IT and risks governance practices as per King IV as well as identified similarities between King IV and other international standards on IT governance and risk disclosure requirements and the likely recommendations aimed at enhancing King IV provisions.

CHAPTER 4: DATA PRESENTATION & ANALYSIS

4.1 Introduction

Information technology is crucial to the effectiveness and efficiency of corporate operations, as was mentioned in the earlier chapters. Furthermore, governance of IT and risk management have become important to an organisation's success, and therefore it is important to evaluate whether organisations comply with the principles and recommended practices of King IV on IT and risk governance and management disclosures. This chapter presents an analysis, and discussion of the results and findings based on the content analysis conducted using the disclosure checklist to assess the extent to which IT risks, governance, and management practices have been disclosed by the top 40 JSE listed entities as recommended by King IV. This section analyses the results and findings to answer the study objectives and research questions and to support the findings and results revealed in previous literature studies.

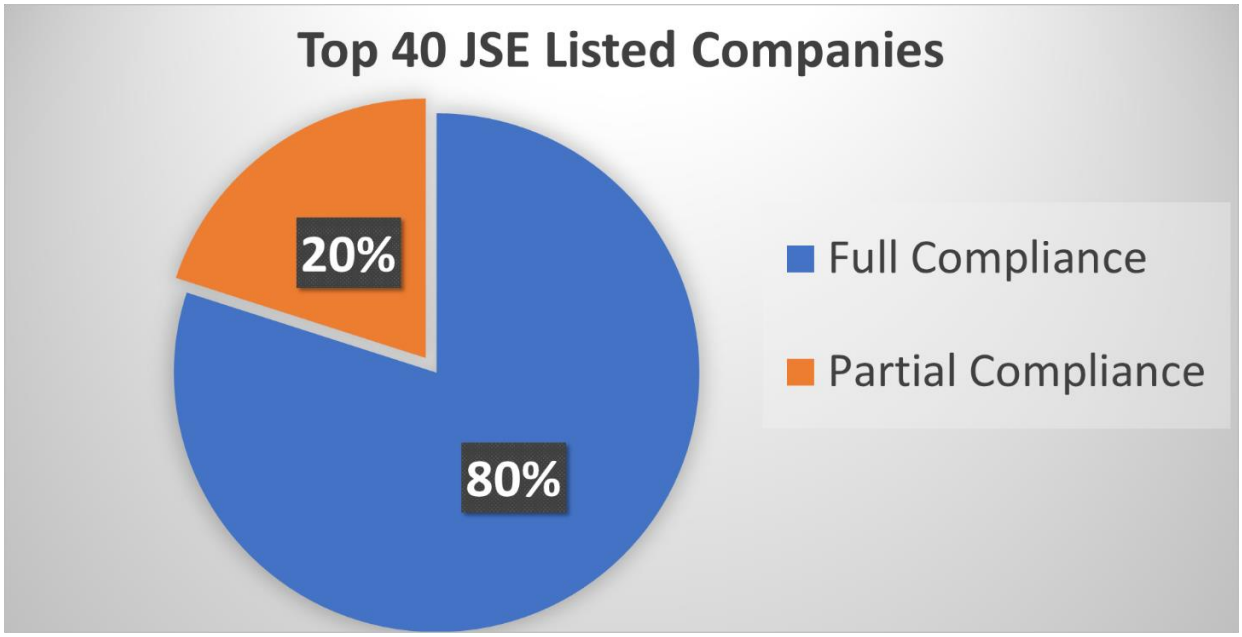
4.2 Results Presentation and Analysis

4.2.1 IT governance and risk management disclosure & King IV application

Overall disclosure results and findings

The evidence for the compliance of JSE top 40 listed entities per King IV's IT governance and risk management is presented in the figure below. According to the overall disclosure results shown in Figure 4.1 below, 32 companies of the top 40 JSE listed entities selected (80%) fully complied with King IV and other international standards including the Johannesburg Stock Exchange, regarding the disclosure of their IT governance and risk management in their integrated and corporate governance reports, whereas 8 companies of the top 40 JSE listed entities selected (20%) partially complied. The results on the King IV's IT governance and risk management disclosure compliance of the top 40 JSE listed companies are therefore consistent with previous studies conducted on King II and III, which indicated that not all companies have fully complied with the previous King principles of corporate governance. Significant improvement was however registered in the current compared to a study by Ngwenya (2015) which identified that 40% of the entities fully met with all King III's IT governance and risk management disclosure requirements whereas 25% partially complied and the remaining 35% did not comply.

Figure 4.1: Overall disclosure on IT governance and risk management

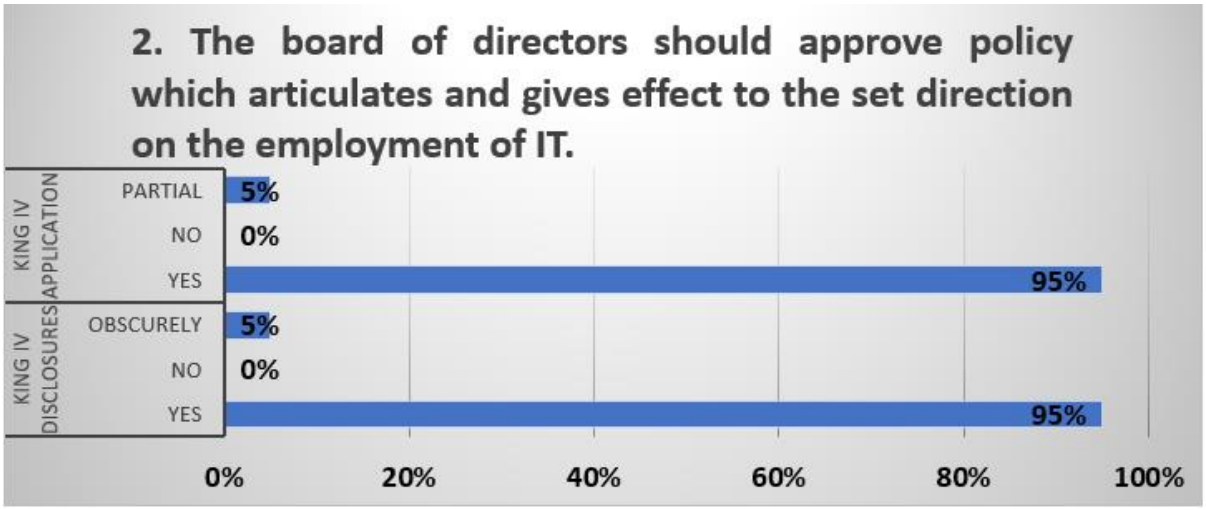


The comprehensive results of the entities examined are listed in Tables 7.1 & 7.2 in Appendix A. The research findings and results presented in Figure 4.1 above are further outlined and a detailed presentation of the actual disclosure and application of King IV on IT governance and risk management are discussed in the sections below.

Figure 4.2: Practice No 1 - IT governance disclosure

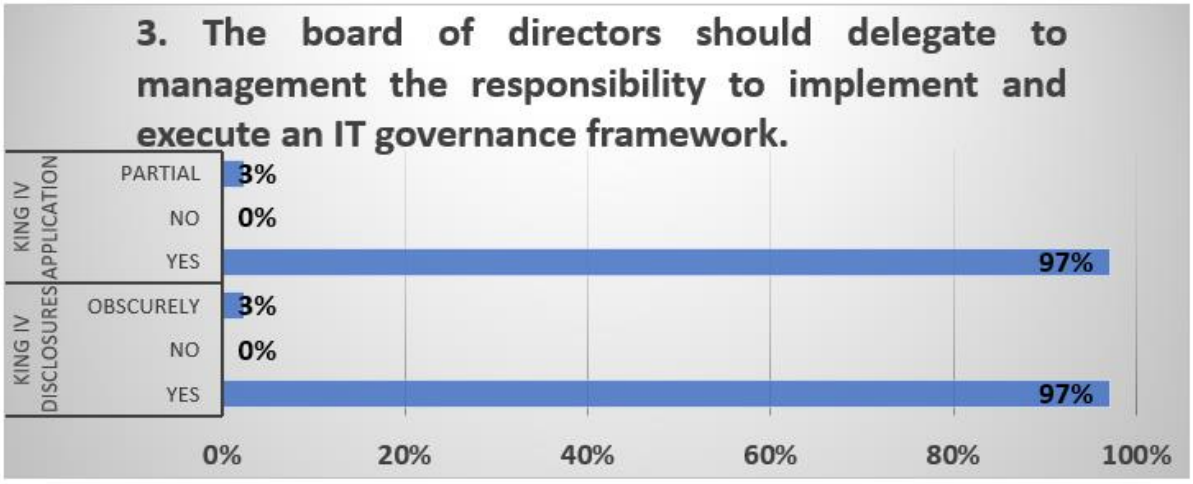
As reflected in Figure 4.2 above, 97% (39 companies) out of the total sampled top 40 JSE-listed companies fully disclosed information relating to the board of directors' responsibility on the governance of IT by providing guidance on how IT should be governed, and they therefore fully complied with King IV. However, 3% (1 company) of the sampled companies were partially compliant with King IV, as they did not provide clear information about the responsibilities of their board of directors on governance of IT.

Figure 4.3: Practice No 2 - IT governance disclosure



As shown in Figure 4.3 above, 95% (38 companies) out of the total sampled top 40 JSE-listed companies fully disclosed information relating to the board of directors' responsibility to approve policies on IT governance and setting direction on the employment of IT; they therefore fully complied with King IV. On the other hand, 5% (2 companies) of the sampled entities did not disclose clear information concerning the board of directors' duty and consequently partly complied with King IV disclosure requirements.

Figure 4.4: Practice No 3 - IT governance disclosure



As indicated in Figure 4.4 above, 97% (39 entities) from the sampled JSE top 40 listed entities fully disclosed information relating to the board of directors' responsibility to delegate to management the tasks relating to the implementation and execution of an IT governance structure; they therefore fully complied with King IV. In contrast, 3% (1 company) of the companies sampled did not provide clear information on board's responsibility, thus partially meeting King IV's requirements.

Figure 4.5: Practice No 4 - IT governance disclosure

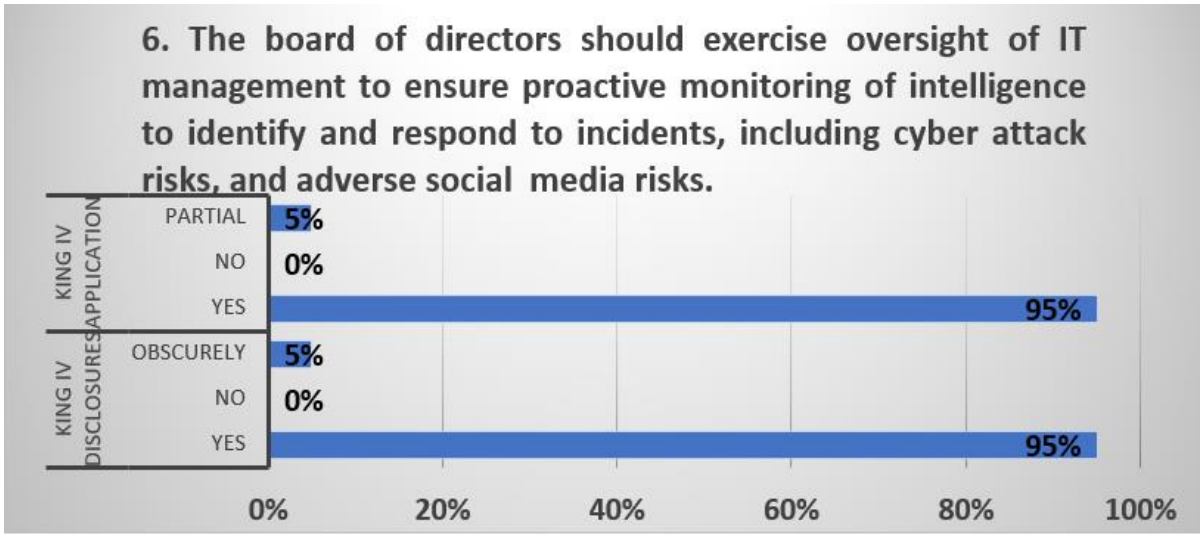
As elaborated in Figure 4.5, above 92% (37 companies) out of the total sampled top 40 JSE-listed companies fully disclosed information relating to the board of directors' responsibility to ensure that IT is in line with the business's performance and sustainability goals, and they therefore fully complied with King IV. However, 8% (3 companies) of the companies sampled were partially compliant with King IV, as they did not provide clear information on board's responsibility to ensure alignment of IT with the performance of the company.

Figure 4.6: Practice No 5 - IT governance disclosure

In Figure 4.6 above, 95% (38 companies) out of the total sampled top 40 JSE-listed companies fully disclosed information relating to the board of directors' responsibility to exercise oversight on IT management to ensure alignment and integration of IT risks into organisation-wide risk management and they therefore fully complied with King IV. However, only

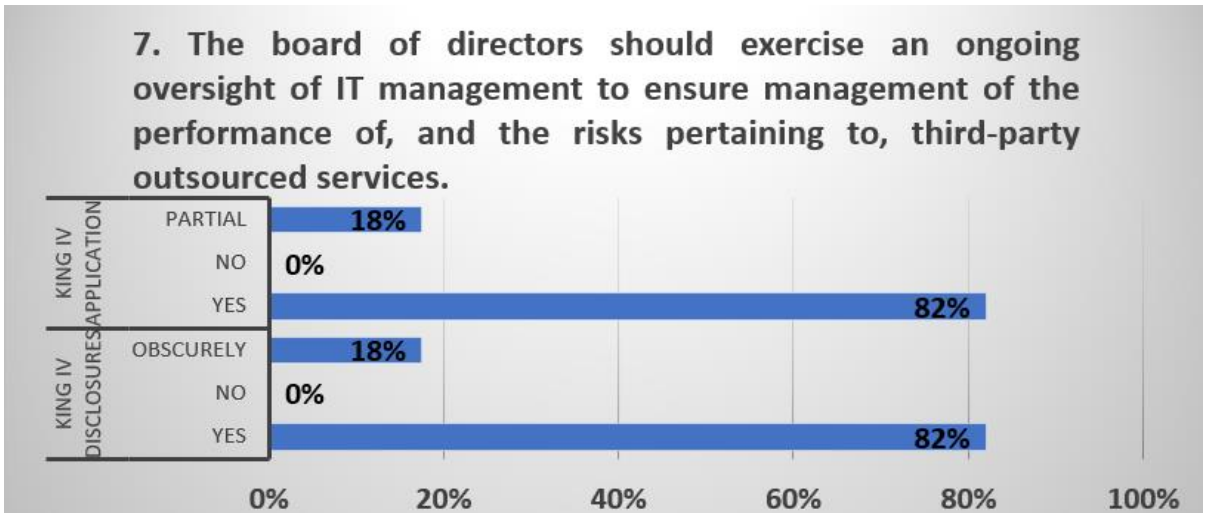
partially complying with King IV was 5% (2 firms) of the sampled companies which did not clearly disclose information relating to the board of directors' oversight responsibility.

Figure 4.7: Practice No 6 - IT governance disclosure



The results in Figure 4.7 above show that 95% (38 companies) out of the total sampled top 40 JSE-listed companies fully disclosed information relating to the board of directors' responsibility to exercise an oversight of IT management aimed at ensuring proactive monitoring, identifying, and responding to incidents which include cyber-attack risks and social media risks and they therefore fully complied with King IV. In contrast, 5% (2 companies) of the sampled companies failed to disclose clear information about the board of directors' responsibility, resulting in only partial compliance with King IV.

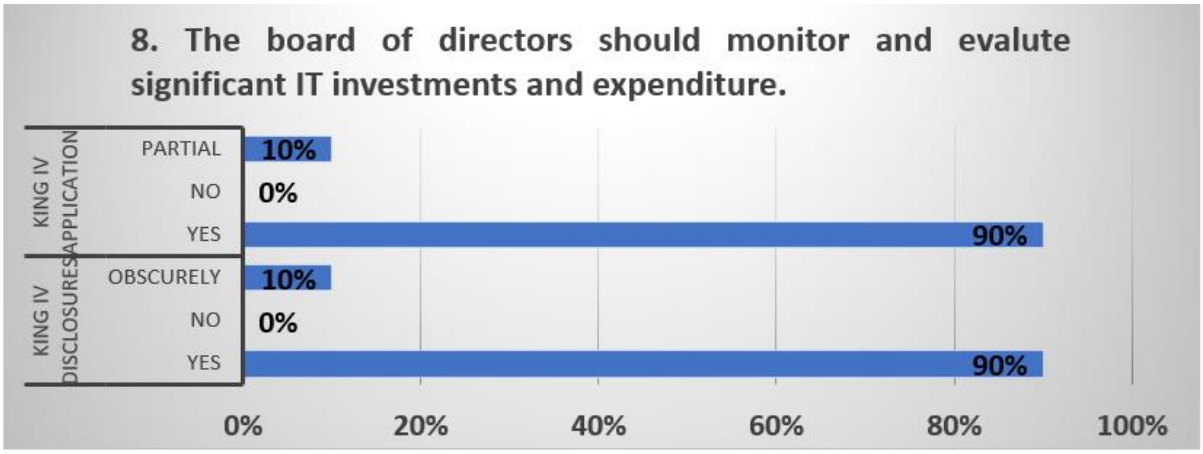
Figure 4.8: Practice No 7 - IT governance disclosure



In light of Figure 4.8 above, 82% (33 companies) out of the total sampled top 40 JSE-listed companies fully disclosed information relating to the board of directors' responsibility to

exercise an oversight of IT management aimed at ensuring the management of performance management and IT risks pertaining to third-party services outsourced services and therefore fully complied with King IV. However, 18% (7 companies) of the examined companies did not publish clearly specific information about the board of directors' responsibility of exercising an oversight to ensure management of IT risks on outsourced services, hence they partially complied with King IV.

Figure 4.9: Practice No 8 - IT governance disclosure



As reflected in Figure 4.9 above, 90% (36 companies) out of the total companies tested fully disclosed information relating to the board of directors' role of monitoring and evaluating significant IT investments and expenditure and therefore they fully complied with King IV. It is however important to note that 10% (4 companies) of the tested companies partly complied with King IV as they did not publish information clearly on the board of directors' responsibility mentioned above.

Figure 4.10: Practice No 9 - IT governance disclosure

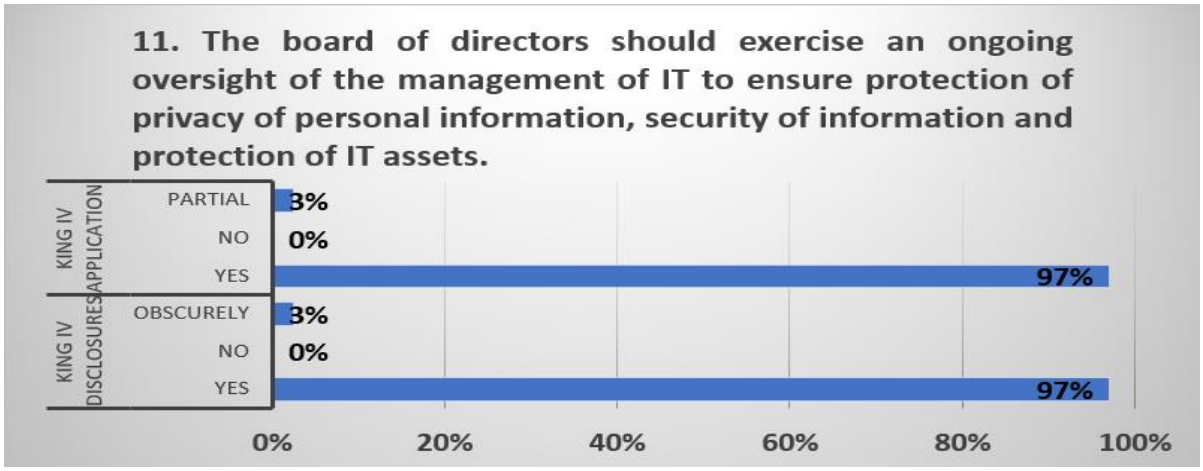
As indicated in Figure 4.10 above, 95% (38 companies) out of the total sampled top 40 JSE-

listed companies fully disclosed information relating to the board of directors' responsibility to exercise an oversight of IT management aimed at ensuring ethics and responsible use of IT and compliance with relevant laws and standards and they therefore fully complied with King IV. However, 5% (2 firms) of the sampled companies did not properly disclose information regarding the board of directors' obligation, and so only partially conformed with King IV.

Figure 4.11: Practice No 10 - IT governance disclosure

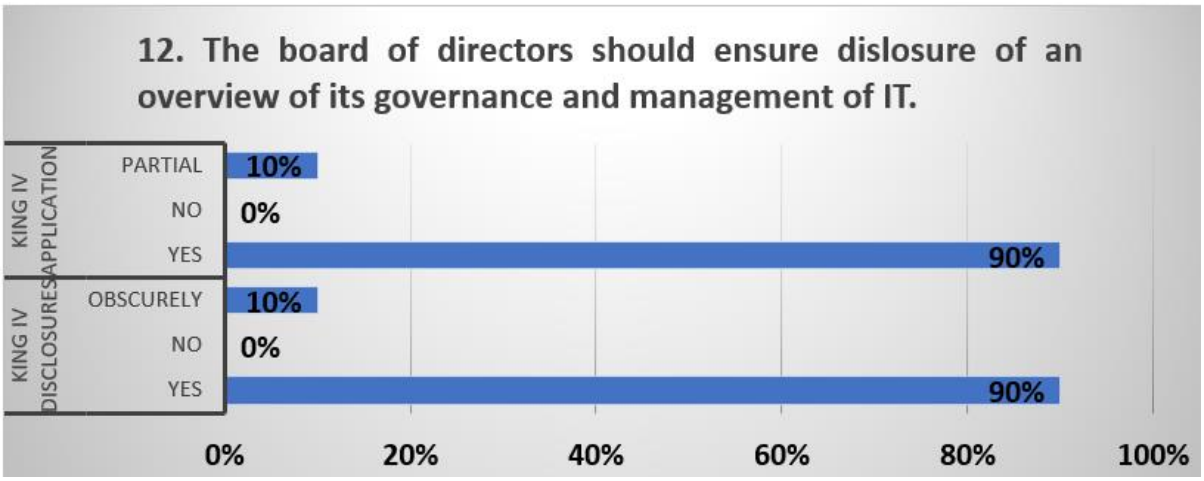
The results in Figure 4.11 above show that 95% (38 companies) out of the total sampled top 40 JSE-listed companies fully disclosed information relating to the board of directors' responsibility to exercise an oversight of IT management aimed at ensuring that IT systems supports confidentiality, integrity and availability of information and they therefore fully complied with King IV. On the other hand, 5% (2 companies) of the selected companies failed to disclose properly information about the board of directors' responsibilities, resulting in only limited compliance with King IV.

Figure 4.12: Practice No 11 - IT governance disclosure



The Figure 4.12 above indicates that 97% (39 companies) out of the total sampled top 40 JSE-listed companies have fully disclosed information relating to the board of directors' responsibility to exercise an oversight of IT management aimed at ensuring protection of privacy of personal information, security of information, and protection of IT assets and they therefore fully complied with King IV. In contrast, 3% (2 companies) of the companies assessed made obscure disclosures about the board of directors' responsibility of ensuring protection and security of personal information and IT assets, thus partially complying with King IV.

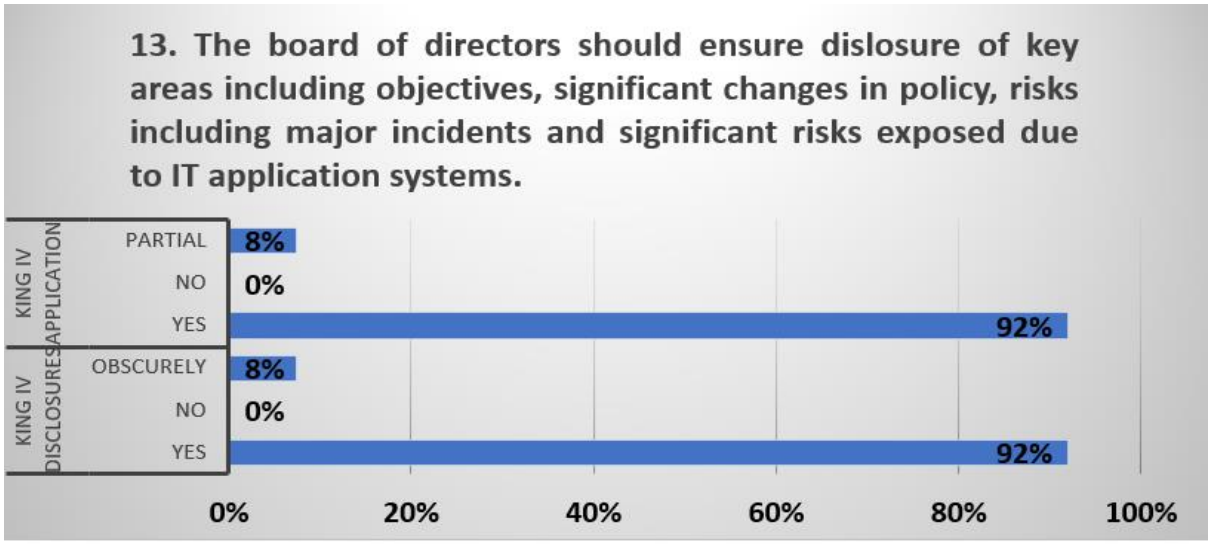
Figure 4.13: Practice No 12 - IT governance disclosure



As shown in Figure 4.13 above, 90% (36 companies) out of the total sampled top 40 JSE-listed companies fully disclosed information relating to the board of directors' responsibility with ensuring the disclosure of an overview of its governance and management of IT and they therefore fully complied with King IV. However, only partially complying with King IV were

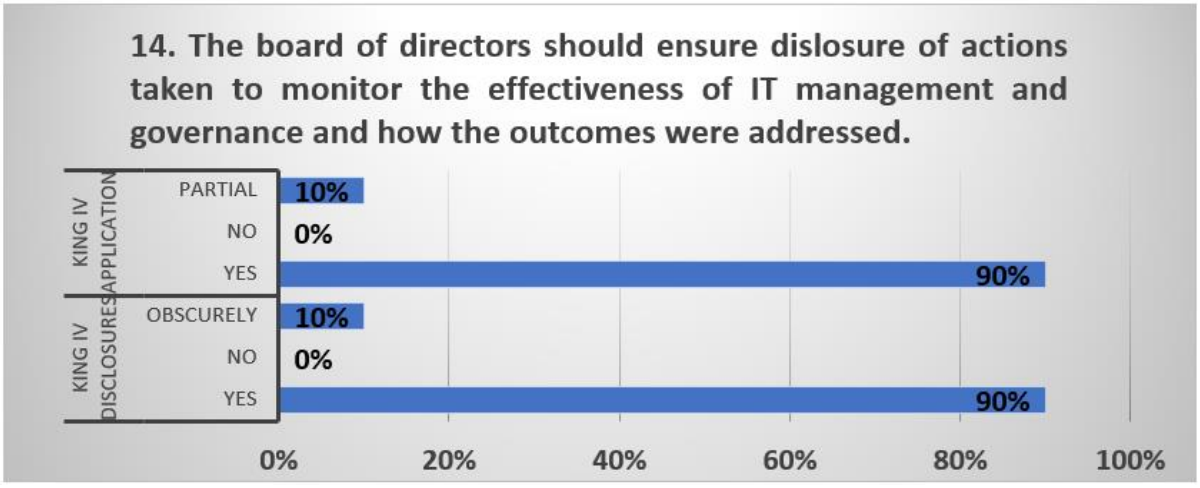
the 10% (4 companies) of the sampled companies that did not properly disclose information on the board of directors' responsibilities.

Figure 4.14: Practice No 13 - IT governance disclosure



Practice number 13 shown in Figure 4.14 above indicates that 92% (37 companies) out of the total sampled top 40 JSE-listed companies fully disclosed information relating to the board of directors' responsibility with ensuring the disclosure of key areas including objectives, significant changes in policy, risks including major incidents and significant risks exposed due to IT application systems. These therefore fully complied with King IV. It is however important to note that 8% (3 companies) of the selected companies failed to clearly disclose information regarding the board of directors' responsibility, thus partially complying with King IV.

Figure 4.15: Practice No 14 - IT governance disclosure



As reflected in Figure 4.15 above 90% (36 companies), out of the total sampled top 40 JSE-

listed companies fully disclosed information relating to the board of directors' responsibility with ensuring the disclosure of key areas including objectives, significant changes in policy, risks including major incidents and significant risks associated with IT application systems and they therefore fully complied with King IV. Even though majority of the companies that were selected conformed fully, 10 % (4 companies) of the companies only partially complied with King IV by failing to publish information on the board of directors' responsibilities in a clear and understandable manner, thus partially complying with King IV.

Figure 4.16: Practice No 15 - Risk governance and management

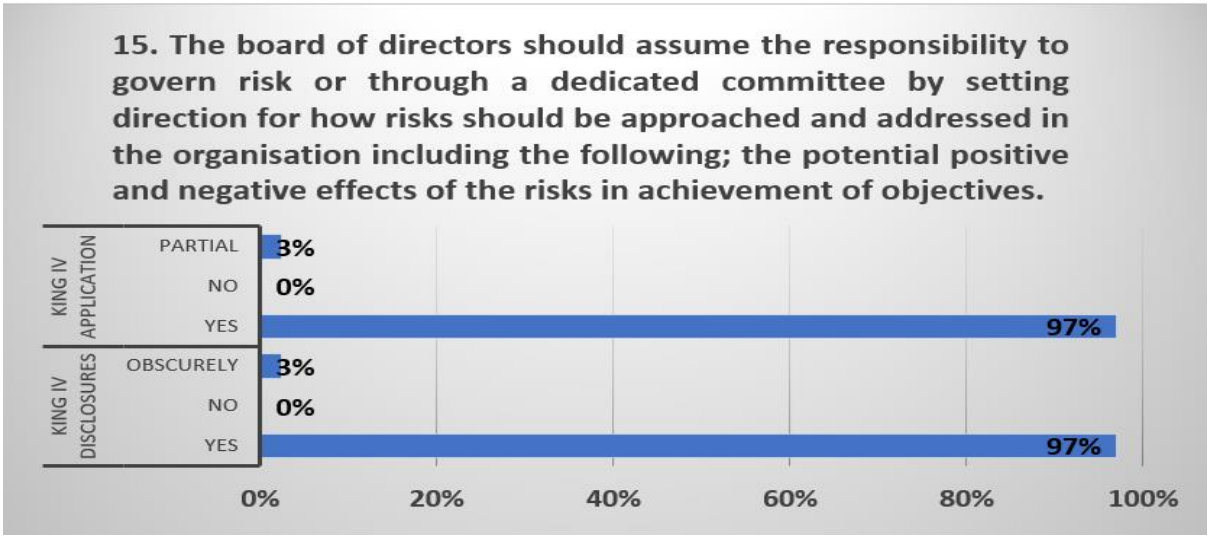


Figure 4.16 above indicates that 97% (39 companies) out of the total sampled top 40 JSE-listed companies fully disclosed information relating to the board of directors' responsibility to govern risk or through a dedicated committee by setting direction for how risks should be approached and addressed in the organisation, and they therefore fully complied with King IV. Nonetheless, just 3% (1 company) of the companies tested failed to clearly disclose information about the board of directors' responsibility, thus partially complying with King IV.

Figure 4.17: Practice No 16 - Risk governance and management

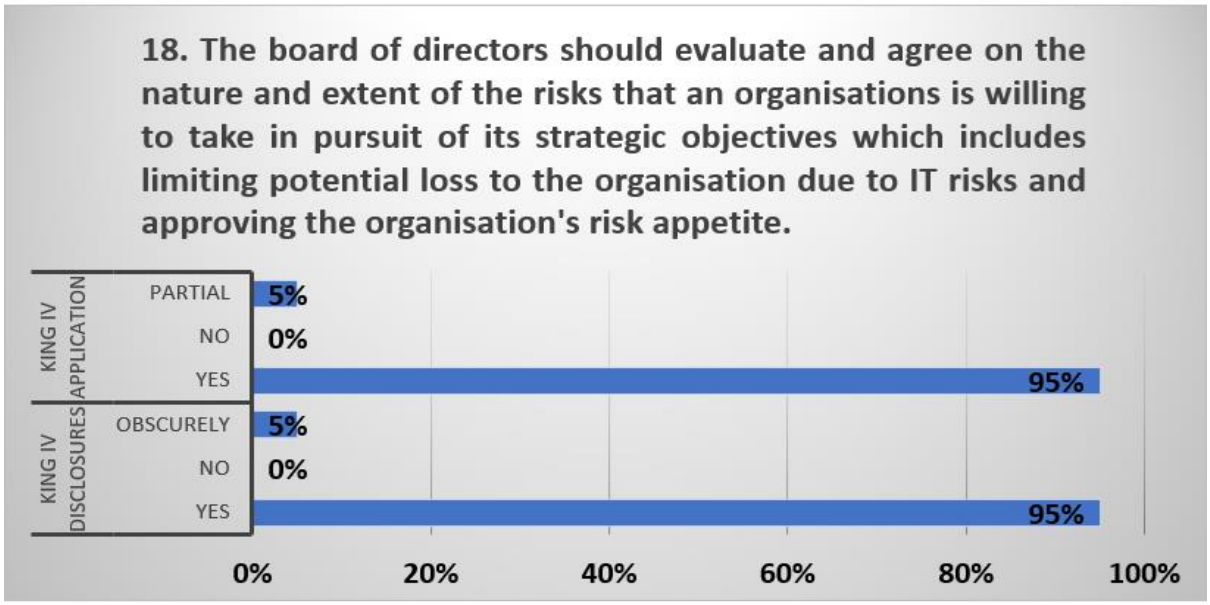
The results shown in Figure 4.17 above indicate that 95% (38 companies) out of the total sampled top 40 JSE-listed companies fully disclosed information relating to the board of directors' responsibility to treat risks as integral in decision making including approval of policies which address the risks and they therefore fully complied with King IV. Nevertheless, 5% (2 companies) of the selected companies did not clearly publish information with respect to the board of directors' duty of managing IT risks; therefore, they partly complied with King IV.

Figure 4.18: Practice No 17 - Risk governance and management

Figure 4.18 above reveals that 97% (39 companies) out of the total sampled top 40 JSE-listed companies fully disclosed information relating to the board of directors' responsibility of delegating to management the task of implementing and executing effective governance and risk management and they therefore fully complied with King IV. However, 5% (1 firm) of the tested companies did not provide a clear disclosure about the board of directors'

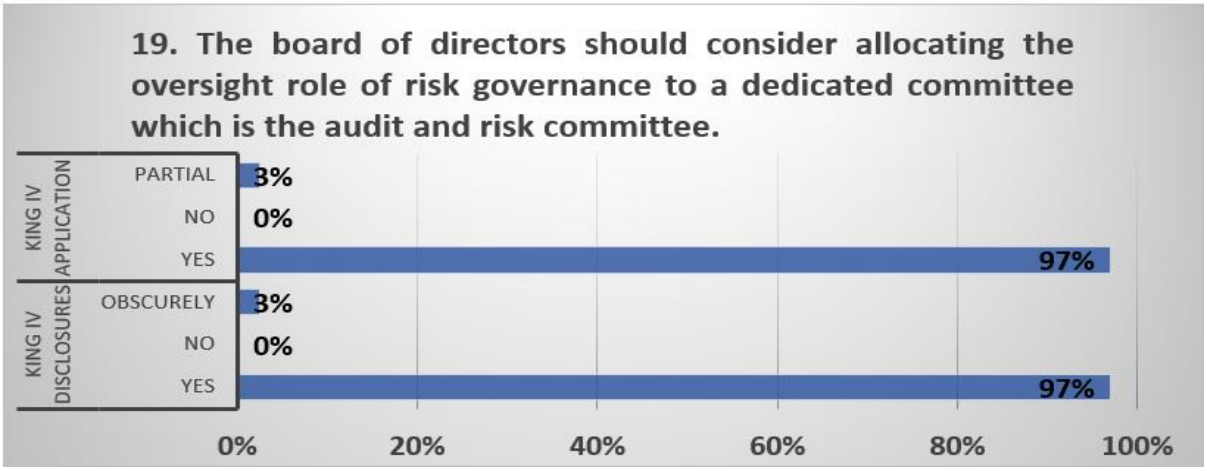
responsibility of delegating risk management to executive management, thus partially complying with King IV.

Figure 4.19: Practice No 18 - Risk governance and management



As reflected in Figure 4.19 above, 95% (38 companies) out of the total sampled top 40 JSE-listed companies fully disclosed information relating to the board of directors' responsibility of evaluating the nature and extent of the risks which an a company is prepared to take to attain the strategic goals including limiting potential loss to the company due to IT risks and approving an organisation's risk appetite and they therefore fully complied with King IV. However, 5% (2 companies) of the assessed companies did not provide clear information and they therefore partially complied with the requirements of King IV.

Figure 4.20: Practice No 19 - Risk governance and management



As elaborated in Figure 4.20 above, 97% (39 companies) out of the total sampled top 40 JSE-

listed companies fully disclosed information relating to the board of directors' responsibility to allocate the oversight role of risk governance to a dedicated committee and they therefore fully complied with King IV. However, 3% (1 company) of the selected companies did not disclose clear information about the board of directors' responsibility above, and thus they partially fulfilled the requirements of King IV.

Figure 4.21: Practice No 20 - Risk governance and management

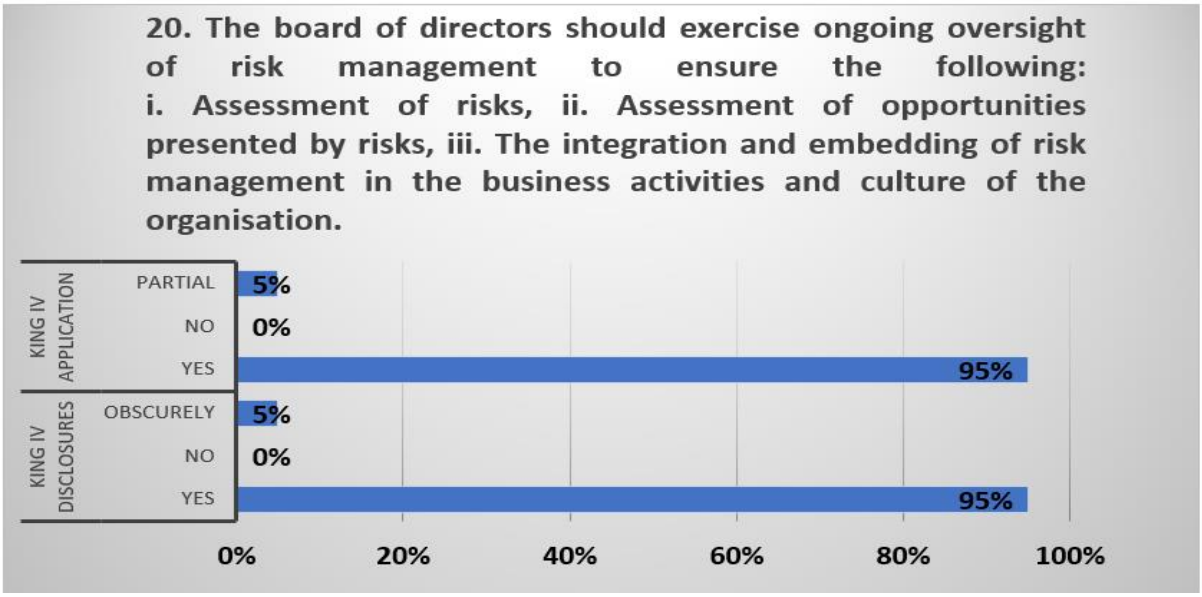
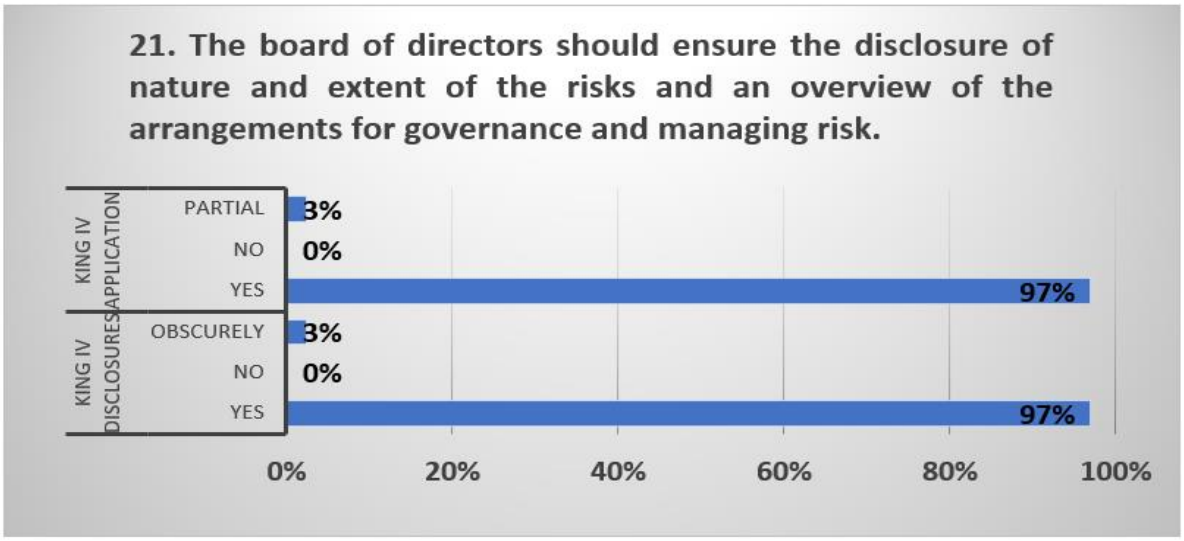


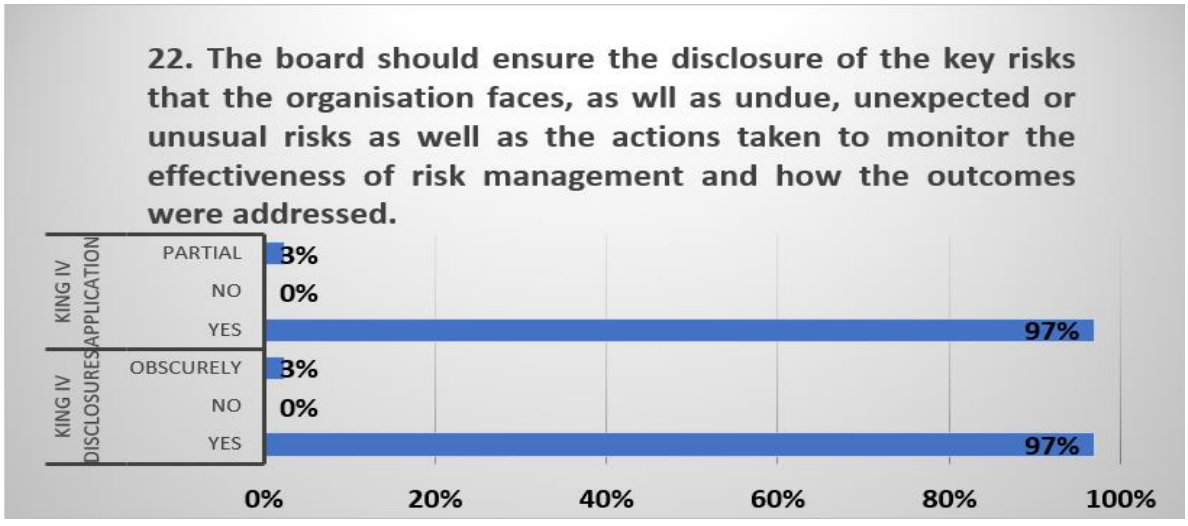
Figure 4.21 above indicates that 95% (38 companies) out of the total sampled top 40 JSE-listed companies fully disclosed information relating to the board of directors' responsibility to exercise an ongoing oversight of risk management including risk assessment and assessment of opportunities presented by the risks and they therefore fully complied with King IV. However, 5% (2 companies) of the sampled companies did not publish clear of information with regards to the board's responsibility and they therefore partially followed King IV.

Figure 4.22: Practice No 21 - Risk governance and management



The results presented in Figure 4.22 above indicate that 97% (39 companies) out of the total sampled top 40 JSE-listed companies fully disclosed information relating to the board's responsibility of ensuring disclosure of the nature and extent of company's risks and an overview of risk governance and management and they therefore fully complied with King IV. In contrast, 3% (1 firm) of the entities assessed failed to provide clear information on the responsibility of the board and hence partially fulfilled the King IV requirements.

Figure 4.23: Practice No 22 - Risk governance and management



As reflected in Figure 4.23 above, 97% (39 companies) out of the total sampled top 40 JSE-listed companies fully disclosed information relating to the board of directors' responsibility of ensuring the disclosure of the key/material risks including unexpected or unusual risks as well as measures undertaken to monitor the effectiveness of risk management and mitigating factors

and they thus fully complied with King IV. However, 3% (1 firm) of the total companies analysed did not provide clear information with regards to the responsibilities of the board of directors and they therefore partially followed King IV.

4.3 Comparison of King IV with other International Standards and regulations on IT governance and risk management disclosure and recommendations to enhance King IV

To ascertain whether the King IV should be enhanced to ensure that it may be clearly understood by the companies and preparers of the integrated and corporate governance reports to ensure competitive advantage as well as effective IT governance risk management and corporate governance, an analysis was conducted aimed at identifying the similarities and differences between King IV and other international standards and regulations on IT governance and risks management disclosure requirements. Table 4.1 below indicates the summary of this comparison.

Table 4 1 : IT governance and risk management disclosure requirements comparison

IT governance & risk management disclosure requirements as per standards, regulations, and Acts	**King IV (IoD, 2016)**	**SOX (SOX Act, 2002)**	**ISA 315 (IASB)**	**ISO 38500/ COBIT 5 (ISO/IEC 38500:2008)**
The board of directors should govern IT in a way that supports the organisation to achieve its strategic objectives (King IV).	√	√	√	√
The board of directors should approve policy which articulates and gives effect to the set direction on the employment of IT (King IV).	√	×	√	√
The board of directors should delegate to management the responsibility to implement and executive an IT governance framework (King IV).	√	×	√	√
The board of directors should exercise an ongoing oversight of IT management to ensure alignment and	√	√	√	√

integration of IT risks into organisation-wide risk management (King IV).				
The board of directors should exercise an ongoing oversight of IT management to ensure proactive monitoring of intelligence to identify and respond to incidents, including cyber-attack risks, and adverse social media risks (King IV).	√	√	√	√
The board of directors should exercise an ongoing oversight of the management of IT to ensure protection of privacy of personal information, security of information and protection of IT assets (King IV).	√	×	√	√
The board of directors should exercise an ongoing oversight of the management of IT to ensure that IT systems support confidentiality, integrity, and availability of information (King IV).	√	√	√	√
The board of directors should exercise an ongoing oversight of IT management to ensure ethical and responsible use of IT and compliance with relevant laws and standards (King IV).	√	√	√	√
The board of directors should monitor and evaluate significant IT investments and expenditure (King IV).	√	×	√	√
The board of directors should ensure disclosure of key areas including				

objectives, significant changes in policy, risks including major incidents and significant risks exposed due to IT application systems (King IV).	√	√	√	√
The board of directors should ensure disclosure of an overview of its governance and management of IT (King IV).	√	√	√	√
The board of directors should ensure disclosure of actions taken to monitor the effectiveness of IT management and governance and how the outcomes were addressed (King IV).	√	√	√	√
The board of directors should treat risks as integral to the way it makes decisions and execute its duties as well as to approve policies which articulates and gives effect to its set direction on risks (King IV).	√	√	√	√
The board of directors should consider allocating the oversight role of risk governance to a dedicated committee which is the audit and risk committee (King IV).	√	√	√	√
The board of directors should evaluate and agree on the nature and extent of the risks that an organisation is willing to take in pursuit of its strategic objectives which includes limiting potential loss to the organisation due to IT risks and approving the organisation's risk appetite (King IV).	√	×	√	√

The board of directors should ensure the disclosure of nature and extent of the risks and an overview of the arrangements for governance and managing risk (King IV).	√	×	√	×
The board of directors should ensure the disclosure of the key risks that the organisation faces, as well as undue, unexpected, or unusual risks as well as the actions taken to monitor the effectiveness of risk management and how the outcomes were addressed. (King IV).	√	×	√	×
Access is authenticated through unique user IDs and passwords or other methods as a mechanism for validating that users are authorised to gain access to the system (ISA 315).	×	√	√	×
Financial data are backed up on a regular basis according to an established schedule and frequency (ISA 315).	×	√	√	×
Management approves the nature and extent of user-access privileges for new and modified user access, including standard application profiles/roles, critical financial reporting transactions, and segregation of duties (ISA 315).	×	√	√	×
Management should establish safeguards aimed at preventing data tampering (SOX 302.2).	×	√	√	×

Management should establish verifiable controls aimed at tracking data access (SOX 302.4B).	×	√	√	×
Management should establish safeguards aimed at ensuring the effectiveness of IT controls (SOX 302.4.D).	√	√	√	√
Management should disclose data security safeguards and data security breaches to enable independent auditors to assess the effectiveness of the internal control structure and security framework (SOX 404 A).	√	√	√	×

Table 4.1 above indicates the similarities and differences between King IV and other international standards and regulations. King IV and all the international standards and regulations agree on some requirements, which include the board of directors' responsibility to govern IT aimed at supporting a company to achieve its strategic objectives, directors responsibility to ensure IT alignment and integration of IT risks into organisation-wide risk management, directors' responsibility to ensure proactive monitoring of risks including cyber-attack risks, directors' responsibility on IT management to ensure that IT systems support confidentiality, integrity and availability of information, directors' responsibility to ensure ethical use of IT and compliance with laws and standards, directors' responsibility to ensure disclosure of an overview of IT governance and risk management as well as disclosure of actions taken to evaluate the effectiveness of IT governance as well as risk management and how outcomes were addressed, directors' responsibility to consider risks as integral to decision making and execution as well as allocating an oversight role of IT risk governance and management to a board committee, mainly the audit and risk committee.

In comparison with International Standards of Auditing (ISA 315) it was revealed that some important requirements relating to IT systems and internal control environment are not included in King IV as well as ISO 38500/COBIT 5, thus resulting in a difference. These requirements include IT security controls through user access and other methods to ensure valid users are allowed to use IT systems and hence preventing these systems from being accessed

by unauthorised users. Management should approve the nature and extent of user-access privileges for new and modified user ingress to prohibit unauthorised access to IT application systems. ISA 315 internal controls require financial data to be backed up regularly in accordance with an established schedule and frequency, which is not indicated in the principles and practices in King IV. To enhance King IV provisions, it is recommended that these requirements on IT systems and internal controls should be integrated into King IV principles of corporate governance.

In comparison with the SOX Act, the study revealed that some important requirements relating to IT application systems and internal control environment are not included in King IV, hence resulting in differences. SOX requires management to establish safeguards aimed at preventing data from tampered with as well as establishing verifiable controls aimed at tracking data access. These principles were not clearly described in the principles and practices in King IV; therefore, to enhance King IV provisions it is recommended that these requirements on IT systems internal controls and safeguards should be incorporated into King IV principles of corporate governance.

4.4 Chapter Summary

The chapter provided a detailed analysis and discussion of the results of King IV IT governance and risk management disclosure compliance by JSE top 40 listed entities. Furthermore, the results relating to the comparison between King IV with other international standards and regulations on IT governance and risk management disclosure requirements were discussed and recommendations for IT governance and risk disclosure that will enhance King IV provisions were proffered.

Regarding IT governance and risk management disclosure and King IV application, the results have indicated that the majority (80%) of the top 40 JSE-listed companies have fully complied and disclosed information about IT governance and risks management and have established IT and risk governance structures such as the audit and risk committee, technology committee, risk management committee, which are mainly tasked with the role of IT governance and risk management. However, the results also revealed that some companies partially complied with King IV IT governance and risk management disclosure and application requirements. A significant improvement was however recognised as previous research on King II and III indicated that A few companies (below 50%) complied with IT governance and risk management disclosure requirements as stipulated in the King codes. The significant

improvement is a sign that the preparers of financial reports, management and boards of companies have understood the principles of King IV code on IT governance and risk management. It is important to note that JSE amended its listing requirements in May 2017 to include a mandatory requirement for listed companies to apply all the King code principles and this contributed to the significant improvement which was revealed in this study. Based on the analysis conducted to compare King IV with other international standards and regulations, it is evident that King IV principles on IT governance and risk management are similar to other international standards and some differences were also noted. Table 4.2 shows a summary and link between findings and literature.

Table 4.2: Relation between findings and literature

No	Research findings	Reference to literature
1.	*To what extent is the JSE top 40 listed entities complying with King IV and other international standards on IT governance and risk disclosure requirements?* Prior research by Janse van Vuuren (2006) on disclosure compliance per King II identified that only 33% of the companies tested fully complied and the remainder did not comply with King II governance and risk disclosure requirements. Furthermore, a similar study by Ngwenya (2015) which focused on King III, revealed that 40% of the JSE top 40 listed companies fully complied with King III, whereas 25% partially complied, and the remaining 35% did not comply with the King III's IT and risk governance disclosure. In addition, Marx et al. (2016) did a study on information technology governance disclosure compliance of JSE top 40 listed companies and revealed that 19 out of 40 companies (47%) were fully compliant, 5 of the 40 companies (15%) were partially compliant and 15 companies (38%) did not comply with King III's IT governance disclosure requirements. It is therefore important to note that from inception of King Code of corporate governance, no study revealed a 100% compliance by companies. Likewise, the current study also revealed a similar trend as only 32 companies (80%) fully complied whereas 8 companies (20%) partially complied with King IV's IT governance and risk disclosure requirements.	(Marx et al., 2016), (Ngwenya, 2015), (van Vuuren, 2006)
2.	*What are the similarities and differences between King IV, International Organisations for Standards (ISO 38500 & COBIT 5), Sarbanes-Oxley Act (SOX), and International Standards of Auditing 315 on IT governance and risk disclosure requirements?* The previous research was conducted by Ngwenya (2015), which compared the similarities and differences between King III and	(Ngwenya, 2015)

	other international standards including SOX and ISA315 on IT governance and risk disclosures. The results indicated that out of the 15 requirements which were used to compare the different standards and code of practices 11 (73%) requirements were similar whereas 4 (27%) requirements were different. Equally so, the current study looked at the similarities and differences between King IV and other international standards including ISO38500, COBIT5, SOX and ISA 315 on IT governance and risk disclosures. The findings from the current study revealed that King IV and other international standards were similar on 19 out of the 24 (79%) of the IT governance and risk management disclosure requirements and differed on 5 out of 24 (21%) requirements.	

A summary and conclusions of the study is provided in the following chapter. It also discusses study's relevance, implications, recommendations, and limitations, and it suggests future research areas.

CHAPTER 5 SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

The primary objective of this study was to assess the extent to which the JSE top 40 listed entities comply with King IV IT governance and risk management disclosures. To accomplish the above aim, a disclosure checklist was developed and used to assess the extent of disclosure. This was done through content analysis. Data were gathered from the annual/integrated reports, analysed, and the results were discussed. Furthermore, the study analysed the similarities and differences between King IV and other international standards and regulations on IT governance and risk management disclosures. Following this, recommendations were provided to enhance King IV provisions. An overall link from chapter 1 to chapter 4 is given, considering all the three study objectives. Then, a conclusion will be drawn based on the results. Finally, suggestions for further research will be made along with the study's limitations and recommendations.

5.2 Summary of the Study

The study's background, the research problem and the research objective were all presented and discussed in the first chapter. This study analysed the extent to which JSE top 40 listed entities comply with King IV and other international standards on IT governance and risks management as well as disclosure on these. In addition, a similarities and differences assessment between King IV and international standards/regulations was conducted and recommendations were provided where King IV principles differed with international standards. A review of literature traced notable academic research which were conducted on company compliance with King II and King III IT governance and risk management disclosure, but there are very few studies which focused on IT governance and risk management disclosures per King IV. The study therefore contributes to literature and provides empirical results on compliance by JSE top 40 listed entities with King IV IT governance and risk management disclosure requirements as well as their application of IT systems to enhance business processes. The recent evidence on corporate governance failures in the case of Steinhoff International Holdings N.V, Tiger Brands Ltd, Tongaat Hulett Ltd which have been marred with corporate scandals in South Africa increased the importance of good governance practices, which among others include effective IT governance and risk management. The major limitation identified in King III's "apply or explain" principle was that promoted a tick box exercise as it was rule-based, with no effective governance. However, the recently adopted King IV philosophy is more outcome based. King IV's "apply and explain" philosophy aims

at ensuring that companies apply the recommended practices and explain their application, in the form of disclosure in the integrated/annual reports, thus promoting effective corporate governance through transparency, fairness and accountability of board and management to its stakeholders.

The first objective of the study was achieved through following a qualitative content analysis approach to the integrated/annual reports together with the King IV guidelines and international standards and regulations. To achieve the study objectives, secondary data in the form of integrated reports, corporate governance reports and sustainability reports were used. A disclosure checklist was designed based on King IV principles 11 and 12 and the recommended practices for effective IT governance and risk management. This was then used to determine whether each company applied full disclosure, non-disclosure or partial disclosure. A qualitative content analysis was therefore performed on the integrated, annual, corporate governance and sustainability reports and statements of the JSE top 40 listed entities to confirm their level of disclosure by each company according to the disclosure checklist. In terms of the second and third objectives the study reviewed the King IV guideline principles and practices against those of ISO standards 38500, Sarbanes-Oxley Act and International Standards of Auditing 315 and identified the similarities and differences in relation to IT governance and risk management.

The results show that 80% of the sampled JSE top 40 listed entities (32 companies) fully complied with King IV IT governance and risk management disclosures in their integrated, annual, corporate governance and sustainability reports. In contrast, 8 companies out of the 40 companies (20%) partially complied with King IV disclosure requirements. A significant improvement has been registered from the current study as compared to previous studies in literature, such as Ngwenya (2015), who indicates that 40% fully complied, 25% partially complied, and 35% did not comply with King III disclosure requirements. It is therefore important to recognise that King IV disclosure guidelines and its outcome-based approach contributed towards good corporate governance and disclosures in comparison with King III, which provided rule-based guidelines. Furthermore, the results indicated that most of King IV principles and recommended practices are similar to those in ISO 38500, Sarbanes – Oxley Act, COBIT 5 and ISA 315, though there were a few practices included in ISA 315 and Sarbanes – Oxley Act which were not identified in King IV guidelines and which resulted in differences. Recommendations were therefore provided to enhance King IV disclosure provisions.

5.3 Key Findings and Implications

The study discussed three objectives, namely assessing the extent to which the top 40 JSE-listed entities conform with King IV on IT governance and risk management disclosures in their annual/integrated reports and corporate governance reports; determining the IT governance and risk disclosure requirements in accordance with King IV and other International Standards, such as ISO 38500, Sarbanes-Oxley Act (SOX), and International Standards of Auditing 315 (ISA 315), and to provide a recommendation to King IV IT governance and risk disclosure requirements following international standards. The following section provides a summary of the key findings, and the implications.

5.3.1 Research objective 1: Assessing the extent to which the JSE top 40 listed entities comply with King IV on IT governance and risk management disclosure requirements in their annual/integrated and corporate governance reports.

To address the objective the following question was drafted;

To what extent is the JSE top 40 listed entities complying with King IV and other international standards on IT governance and risk disclosure requirements?

The results revealed that 32 companies, which represent 80% of the sampled top 40 JSE listed entities, fully complied with King IV's and other international standards including the Johannesburg Stock Exchange listing requirements on the disclosure of their IT governance and risk management in the annual/integrated and corporate governance reports. However, 8 companies that represent 20% of top 40 JSE listed companies partially complied. This study shows a significant improvement compared to the previous study by Ngwenya (2015), which revealed that 40% fully complied with King III, whereas 25% partially complied, and the remaining 35% did not comply with the King III's IT governance and risk management disclosure. The substantial improvement on entities' disclosures as required by King IV can also be linked to its simplified principles and recommended practices of "Apply and Explain" as compared to the previous King III's "Apply or Explain". The King IV's "Apply and Explain" concept outlined that all the principles and recommended practices applied by a company should be supported by a detailed disclosure on how it was applied, whereas King III's "Apply or Explain" concept required a company to apply the code's practices and, if not, explain why the recommended practices did not apply to the company (IoD, 2016). In addition, the recently adopted King IV code is outcome-based as compared to King III's rule based;

King IV focuses on application of principles and practices and disclosure of these rather than enforcing rules of application.

5.3.2 Implication of Findings

Full compliance with IT governance and risk management disclosure is beneficial to shareholders, potential investors, and other stakeholders as IT governance and risk management is an important factor for consideration before undertaking an investment. Effective IT governance and risk management practices enable a company to reduce going concern risk, thus benefiting employees with guaranteed employment, growth in revenue and income for the company, which may also result in an increase of the share price and shareholders' returns as well as the South African economy through company contributions in the form of taxation and employment creation. Good practice of corporate governance yields good performance, effective application of control risk management and financial reporting which boosts confidence in potential investors to invest in the company, thus pushing the stock prices high. Full compliance with King IV IT governance and risk management may result in an enhanced credibility and reputation to the company, which enables it to attract investors/shareholders and raise more capital as well as potential growth as it will attract customer support, loyalty and retention of talented employees.

Effective IT governance, risk management and good controls contribute to preventing fraud and data losses. Full disclosure compliance enhances transparency, integrity, fairness and accountability which increases confidence by the stakeholders which may result in increased growth. Furthermore, compliance with IT governance and risk management practices and disclosure prevents a company from potential regulation and law breaches, which may result in fines and penalties mainly because part of the JSE listing requirements includes full compliance with King IV.

5.3.3 Research objective 2: Determining the IT governance and risk disclosure requirements in accordance with King IV and other International Standards (ISO 38500), Sarbanes-Oxley Act (SOX), and International Standards of Auditing 315 (ISA 315).

In addressing the objective, the question below was asked;

What are the similarities and differences between King IV, International Organisations for Standards (ISO 38500 & COBIT 5), Sarbanes-Oxley Act, and International Standards of Auditing 315 on IT governance and risk disclosure requirements?

The results indicated that there are similarities and differences between King IV and other international standards and regulations. Some of the requirements in which King IV is similar to other international standards and regulations which were identified include the following:

- Board of directors' responsibility to govern IT aimed at supporting a company to achieve its strategic objectives;
- Board of directors' responsibility to ensure IT alignment and integration of IT risks into company-wide risk management;
- Board of directors' responsibility to ensure proactive monitoring of risks, which include risks of cyber-attacks which is on the rise owing to adoption of artificial intelligence methods and an increase in the use of technology systems by companies;
- Board of directors' responsibility to ensure that IT systems support confidentiality, integrity, and availability of information;
- Board of directors' responsibility to ensure ethical use of IT and compliance with laws and standards;
- Board of directors' responsibility to ensure disclosure of an overview of IT governance and risk management as well as disclosure of actions taken to monitor the effectiveness of IT governance and risk management and how the outcomes were addressed;
- Board of director's responsibility to ensure that risks are treated as integral in decision making and execution as well as delegating an oversight role of IT risk governance and management to a dedicated committee such as the audit and risk committee.

Some of the requirements in which King IV is different from other international standards and regulations are the following:

- International Standards of Auditing (ISA 315) requires effective IT security controls through user access and other methods which are aimed at ensuring that only valid users gain access to the IT application systems and thus preventing the systems from being accessed by unauthorised users;
- With ISA 315, management is required to approve the nature and extent of user-access privileges for new and modified user access to prohibit unauthorised access to IT application systems;
- ISA 315 requires financial data to be backed up regularly in accordance with an established schedule and frequency; these are not indicated in King IV principles and recommended practises on IT governance and risk management;

- Sarbanes-Oxley Act (SOX) requires management to establish safeguards which are aimed at preventing data from being tampered with as well as to establish verifiable controls which are aimed at tracking data access. These principles are not indicated in King IV principles and recommended practises on IT governance and risk management.

The above section articulated similarities and differences between KING IV and other international standards and regulations. Similarities show consensus with regulations of IT governance and risk management. The differences may be attributed to many reasons, such as differences in specific country regulations, differences in risks which may be country specific.

5.3.4 Implications of Findings

The study identified that most of the JSE top 40 listed entities are multinational companies and hence they have operations in other countries outside South Africa. King IV code of corporate governance was designed by the Institute of Directors South Africa with the aim of promoting good governance practices. Because most of the entities are multinational, it is important for good governance practices to be applied internationally. Furthermore, it is important to note that most of the King IV principles and recommended practices regarding IT governance and risk management were aligned with the international standards and regulations such as ISO 38500, COBIT 5, SOX, and ISA 315. The alignment is of great importance as it contributes towards effective IT governance by the multinational companies in their operations globally. Alignment of the King IV principles and practises with international standards on IT governance and risk management increases multi- stakeholders' ability to interpret the IT governance and risk management disclosures. Similar principles and practises ensure uniformity and consistency application from company to company, thus enabling preparers of annual reports to apply, explain and disclose IT governance and risk management practices. By aligning King IV principles with international standards, multinational companies listed on JSE are able to comply with laws and standards in other countries. Entities with operations in the United States of America are required by the Sarbanes-Oxley Act to disclose compliance on data loss prevention, data safeguards, data security and effective internal controls and data security frameworks; hence, applying King IV principles, which is internationally aligned, reduces non-compliance and liabilities associated fines and penalties.

In addition, the study revealed that some principles and best practises applied in the international standards and regulations have not been integrated in the recently developed King IV code of good corporate governance. The identified differences, which were not incorporated

into King IV, mainly related to IT systems access, controls, financial data security, access controls and safeguards on financial data from being accessed by authorised users. The implications of non-alignment on these best practices may result in non-compliance in other countries by the multinational companies which may have financial implications in the form of fines, penalties, and potential legal claims on incidences of data breach.

5.3.5 Research objective 3: Providing a recommendation to King IV IT governance and risk disclosure requirements following international standards (ISO 38500 & COBIT 5), Sarbanes-Oxley Act (SOX), and ISA 315 clarifies disclosure requirements to South African companies that are required to comply with King IV.

Concerning the similarities and differences between King IV and other international standards, the results have shown that King IV principles and recommended practises on IT governance and risk management did not include the following practises and guidelines which were included in ISA 315 and Sarbanes-Oxley Act, which mainly relate to internal control:

- Board of directors' responsibility of oversight to ensure effective IT security controls through user access and other methods which are aimed at ensuring that only valid users gain access to the IT application systems and thus preventing the systems from being accessed by unauthorised users;
- Management should approve the nature and extent of user-access privileges for new and modified user access aimed at prohibiting unauthorised access to IT application systems;
- Management responsibility of ensuring that financial data are backed up regularly in accordance with an established schedule and frequency, and
- Management responsibility to establish safeguards which are aimed at preventing data from being tampered with as well as to establish verifiable controls which are aimed at tracking data access.

It is therefore recommended that board oversight responsibility and disclosure on the IT systems and internal controls, which includes IT security controls in the form of user access, valid user access, approval of user-access privileges and prohibition of unauthorised users on IT systems should be incorporated into King IV to enhance its provision on corporate governance. In addition, it is further recommended that King IV should also incorporate into its principles the management responsibility of ensuring financial data backups regularly,

safeguards of data to prevent tampering and unauthorised access as well as establishment of verifiable controls to track data.

Furthermore, the study results indicated that there are companies which have not fully adhered to the principles and recommended practices in King IV with regards to IT governance risk management practises. It is therefore recommended that a framework should be designed to provide clear guidelines on what information must be disclosed in the annual reports of an organisation in respect to IT governance and risk management practices to ensure uniformity and consistency of application from company to company. Clear guidelines enable the preparers of the integrated/annual reports to apply and explain as well as disclose important information relating to IT governance and risk management. As a result, it would be easier for stakeholders to understand the disclosures on IT governance and risk management in the integrated reports.

5.4 Conclusion

IT has become a critical resource for all companies, and it assists in the collection and processing of information as well as supporting businesses to achieve their strategic objectives. IT therefore plays the most vital role in a company's operations. The increase in use of IT applications systems has however exposed companies to new risks, which require effective IT governance and risk management to safeguard a company's data. Literature revealed different types of IT risks, which are exposed to companies, and which include cyber-attacks, data breaches, IT system failure, social media risks, malware, IT data security risk, and integrity risks among risks. These risks expose a company to extensive financial loss as well as loss of key information, which can result in extensive reputational damage, legal claims and loss of stakeholder confidence, thus affecting the company's going concern ability. Cyber- attacks, which include ransomwares and malwares, result in loss of financial records and loss of customer data, thus impacting future operations and cashflow generation of the company and its going concern ability. Furthermore, IT system failures may halt continued business operations that result in loss of revenue, customers and increase in operating costs, thus affecting a company's going concern ability. The risks identified above therefore require effective IT risk governance and management, which aims to reduce the IT related risks and disclosure of these risks. Company risk management approach in the integrated/annual reports was identified to be critical as it enables stakeholders to understand how IT resources have

been used and how IT risks have been monitored and controlled to achieve a company's strategic objectives.

Most of the companies sampled in this study disclosed their IT risks as well as risk management and governance approach in their integrated reports, whilst a few partially disclosed their IT risks and risk governance approach. The study also revealed that there are similarities and differences between King IV and other international standards and regulations. The main differences identified relate to IT internal controls and security of financial information; therefore, recommendations are provided to enhance King IV provisions on IT governance and risk management disclosure. The study contributes to literature on corporate governance reporting by public companies and to debates on IT governance and risk disclosures.

5.5 Limitation of the study

King IV provides guidelines and principles, but it lacks legal authority to compel adoption and disclosures required. It only relies on the regulatory institutions to enforce its principles and practises. In addition, the research was limited by the fact that King IV only became effective years after 1 April 2017 and hence relevant publications are still limited.

5.6 Suggested future research

The research only concentrated on the JSE top 40 listed companies. It is recommended that future studies focus on the whole JSE main board as a follow up to these results, to examine whether there will be consistency or contradiction with the results of this study. Furthermore, future research studies can also focus on investigating the difficulties that companies experience, which can prevent them from providing a full and clear disclosure of IT risks and their governance and risk management practises in the integrated and annual reports. In addition, a study may focus on developing a framework which provides a clear application guideline on what should be incorporated in the entity's annual reports in respect of disclosure of IT risk, governance, and risk management practises to ensure uniformity and consistency.

6. REFERENCES

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

Abraham, S., & Shrives, P. J. (2014). Improving the relevance of risk factor disclosure in corporate annual reports. The British accounting review, 46(1), 91-107.

Act, S.-O. (2002). Sarbanes-oxley act. Washington DC.

Adams, C. A. (2015). The international integrated reporting council: a call to action. Critical Perspectives on Accounting, 27, 23-28.

Ahuja, S., & Chan, Y. E. (2015). IT Security Governance: A Framework based on ISO 38500. CONF-IRM,

Al-Rahamneh, L. S. (2016). The impact of computerized information systems on the compliance of internal control requirements according to ISA (315) in Jordanian Companies from the perspectives of their employees. International Journal of Economics and Finance, 8(9), 156-172.

Alkebsi, M., & Aziz, K. A. (2017). Information technology usage, top management support and internal audit effectiveness. Asian Journal of Accounting and Governance, 8(1), 123-132.

Alkebsi, M., Aziz, K. A., Mohammed, Z. M., & Dhaifallah, B. (2014). The Relationship Between Information Technology Usage, Top Management Suppport And Internal Audit Effectiveness. International Management Accounting Conference,

Baker, C., Rajaratnam, K., & Flint, E. J. (2016). Beta estimates of shares on the JSE Top 40 in the context of reference-day risk. Environment Systems and Decisions, 36(2), 126-141.

Barr, G., Kantor, B., & Holdsworth, C. (2007). The effect of the rand exchange rate on the JSE Top-40 stocks-an analysis for the practitioner. South African Journal of Business Management, 38(1), 45-58.

Bell, E., Bryman, A., & Harley, B. (2018). Business research methods. Oxford university press.

Bell, E., Harley, B., & Bryman, A. (2022). Business research methods. Oxford university press.

Bellamy, C. (2011). Principles of methodology: Research design in social science. Sage.

Bhat, A., Bennett, I. M., Bauer, A. M., Beidas, R. S., Eriksen, W., Barg, F. K., Gold, R., & Unützer, J. (2020). Longitudinal remote coaching for implementation of perinatal collaborative care: a mixed-methods analysis. Psychiatric Services, 71(5), 518-521.

Boesso, G., & Kumar, K. (2007). Drivers of corporate voluntary disclosure: A framework and empirical evidence from Italy and the United States. Accounting, Auditing & Accountability Journal, 20(2), 269-296.

Brisebois, R., Boyd, G., & Shadid, Z. (2007). What is IT Governance and Why is it Important. 5th Performance Seminar of the INTOSAI IT Standing Committee,

Brown, W., & Nasuti, F. (2005a). Sarbanes-Oxley and enterprise security: IT governance-what it takes to get the job done. Inf. Secur. J. A Glob. Perspect., 14(5), 15-28.

Brown, W., & Nasuti, F. (2005b). What ERP systems can tell us about Sarbanes-Oxley. Information Management & Computer Security.

Bryman, A. (2003). Research methods and organization studies. Routledge.

Byrnes, P., Gullvist, B., Brown-Liburd, H., Teeter, R., Mcquilken, D., & Vasarhelyi, M. (2012). Evolution of Auditing: From the Traditional Approach to the Future Audit-White Paper. American Institute of Certified Public Accountants (AICPA), New York.

Castelo Branco, M., & Lima Rodriques, L. (2007). Positioning stakeholder theory within the debate on corporate social responsibility. EJBO-Electronic Journal of Business Ethics and Organization Studies. Journal, 12 (1), 1-11.

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.
Clark, V. L. P., & Creswell, J. W. (2008). The mixed methods reader. Sage.
Curtin, D. P. (1998). Information technology: The breaking wave. Irwin Professional Publishing.
De Haes, S., Joshi, A., Huygh, T., & Jansen, S. (2017). Exploring how corporate governance codes address IT governance. ISACA Journal, 4, 1-7.
De Haes, S., & Van Grembergen, W. (2008). Practices in IT governance and business/IT alignment. Information Systems Control Journal, 2(2008), 1-5.
De Haes, S., & Van Grembergen, W. (2015). Enterprise governance of information technology. Achieving alignment and value, featuring COBIT, 5(1), 1-10.
De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. Journal of Information Systems, 27(1), 307-324.
De Villiers, C., Rinaldi, L., & Unerman, J. (2014). Integrated Reporting: Insights, gaps and an agenda for future research. Accounting, Auditing & Accountability Journal. Journal, 27 (7), 1042-1067.
Debreceny, R. S. (2013). Research on IT governance, risk, and value: Challenges and opportunities. Journal of Information Systems, 27(1), 129-135.
Dhillon, G., & Mishra, S. (2006). The impact of the Sarbanes-Oxley (SOX) act on information security. Enterprise information systems assurance and system security: managerial and technical issues, 62-79.
Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security, 4(2), 92-100.
Donaldson, T., & Preston, L. E. (1995). The stakeholder theory of the corporation: Concepts, evidence, and implications. Academy of management Review, 20(1), 65-91.
Dumay, J., Bernardi, C., Guthrie, J., & Demartini, P. (2016). Integrated reporting: A structured literature review. Accounting forum,
Elazhary, M., Popovič, A., Henrique de Souza Bermejo, P., & Oliveira, T. (2022). How Information Technology Governance Influences Organizational Agility: The Role of Market Turbulence. Information Systems Management, 1-21.
Freeman, R. E., & Reed, D. L. (1983). Stockholders and stakeholders: A new perspective on corporate governance. California management review, 25(3), 88-106.
Freeman, R. E., Wicks, A. C., & Parmar, B. (2004). Stakeholder theory and "the corporate objective revisited". Organization science, 15(3), 364-369.
Gheorghe, M. (2010). Audit Methodology for IT Governance. Informatica Economica, 14(1).
Haes, S. D., & Grembergen, W. V. (2015). Enterprise Governance of IT. In Enterprise Governance of Information Technology (pp. 11-43). Springer.
Hall, J. A., & Liedtka, S. L. (2007). The Sarbanes-Oxley Act: implications for large-scale IT outsourcing. Communications of the ACM, 50(3), 95-100.
Hardy, G. (2005). Information Risks: Whose business are they. IT Governance institute.
Hendry, J. (2001). Missing the target: Normative stakeholder theory and the corporate governance debate. Business Ethics Quarterly, 159-176.
Hohls-du Preez, C. (2016). IT risk management disclosure in the integrated reports of the Top 40 listed companies on the JSE Limited. University of Johannesburg (South Africa). (Masters Dissertation, University of Johannesburg).
Hudson, L. A., & Ozanne, J. L. (1988). Alternative ways of seeking knowledge in consumer research. Journal of consumer research, 14(4), 508-521.
IoD. (2016). King IV report on corporate governance in South Africa. Africa, LNS.

James, M. L. (2014). THE BENEFITS OF SUSTAINABILITY AND INTEGRATED REPORTING: AN INVESTIGATION OF ACCOUNTING MAJORS'PERCEPTIONS. Journal of Legal, Ethical and Regulatory Issues, 17(2), 93.
Jordaan, W. (2019). IT Governance Disclosure Practices in the Annual Integrated Reports of South African Listed Companies. University of Johannesburg (South Africa). (Masters Dissertation, University of Johannesburg)
Juiz, C., Guerrero, C., & Lera, I. (2014). Implementing good governance principles for the public sector in information technology governance frameworks. Open Journal of Accounting, 2014, 3(1), 9-27.
Kim, N.-y., Robles, R. J., Cho, S.-E., Lee, Y.-S., & Kim, T.-h. (2008). SOX act and IT security governance. 2008 International Symposium on Ubiquitous Multimedia Computing,
Kotze, A. (2017). FTSE/JSE Top 40 index long-term returns. Available at SSRN 2978093.
Leedy, P. D., Ormrod, J. E., & Johnson, L. R. (2014). Practical research: Planning and design. Pearson Education.
Levstek, A., Hovelja, T., & Pucihar, A. (2018). IT governance mechanisms and contingency factors: Towards an adaptive IT governance model. Organizacija, 51(4), 286-310.
Madrigal, M. H., Guzmán, B. A., & Guzmán, C. A. (2015). Determinants of corporate risk disclosure in large Spanish companies: a snapshot. Contaduría y administración, 60(4), 757-775.
Mamaro, L. P., & Tjano, R. (2019). The relationship between dividend payout and financial performance: evidence from Top40 JSE firms. The Journal of Accounting and Management, 9(2).
Mangalaraj, G., Singh, A., & Taneja, A. (2014). IT governance frameworks and COBIT-a literature review.
Maree, K., & Van der Westhuizen, C. N. (2009). Head start in designing research proposals in the social sciences. Juta and Company Ltd.
Mariri, T., & Chipunza, C. (2011). Corporate governance, corporate social responsibility and sustainability: Comparing corporate priorities within the South African mining industry. Journal of human ecology, 35(2), 95-111.
Marx, A., Moolman, A., & Ngwenya, M. (2016). Information technology governance disclosure compliance of JSE-listed companies. International Journal of eBusiness and eGovernment Studies, 8(1), 57-70.
Marx, B. (2009). An analysis of audit committee responsibilities and disclosure practices at large listed companies in South Africa. South African Journal of Accounting Research, 23(1), 31-44.
Marx, B., & Hohls-du Preez, C. (2017). IT RISK MANAGEMENT DISCLOSURE IN THE INTEGRATED REPORTS OF THE TOP 40 LISTED COMPANIES ON THE JSE LIMITED. institutions, 7(3), 27-34.
Marx, B., & Mohammadali-Haji, A. (2014). Emerging trends in reporting: an analysis of integrated reporting practices by South African top 40 listed companies. Journal of Economic and Financial Sciences, 7(1), 231-250.
Marx, B., & Voogt, T. (2010). Audit committee responsibilities vis-á-vis internal audit: how well do Top 40 FTSE/JSElisted companies shape up? Meditari Accountancy Research.
Mohamad, S., & Toomey, M. (2016). A survey of information technology governance capability in five jurisdictions using the ISO 38500: 2008 framework. International Journal of Disclosure and Governance, 13(1), 53-74.
Moloi, T., Nharo, T., & Hlobo, M. (2021). The relationship between board characteristics and dividend payment policies: The JSE Top 40 listed companies cases. Journal of Academic Finance, 12(1), 30-52.

Moolman, A., & Ngwenya, M. KING III INFORMATION TECHNOLOGY GOVERNANCE REQUIREMENTS–AN INTERNATIONAL COMPARISON. International Journal of eBusiness and eGovernment Studies, 8(2), 34-46.

Moolman, J., Oberholzer, M., & Steyn, M. (2016). The effect of integrated reporting on integrated thinking between risk, opportunity and strategy and the disclosure of risks and opportunities. Southern African Business Review, 20(1), 600-627.

Mosiane, P. T. (2018). An analysis of risk management disclosure in the consumer goods sector North-West University (South Africa). Potchefstroom Campus]. (Masters Dissertation, North-West University).

Muslih, M., Sugianti, I., Simanjuntak, D. F., & Rahadi, D. R. (2020). The Effect of Information Technology Governance and Enterprise Risk Management on the Performance of State-Owned Enterprises in Non-Public Financial Fields Moderated by Corporate Governance. International Journal of Science and Society, 2(4), 446-466.

Ngwenya, M. (2015). Analysing information technology governance disclosure of the top 40 JSE listed companies. (Masters Dissertation, North-West University)

O'Brien, J. A. (1996). Management information systems: managing information technology in the networket enterprise.

Obalola, M. (2008). Beyond philanthropy: corporate social responsibility in the Nigerian insurance industry. Social responsibility journal. Journal., 4(4), 538-548.

Pa, N. C., BOKOLO JNR, A., Nor, R. N. H., & Murad, M. A. A. (2015). Risk assessment of IT governance: A systematic literature review. Journal of Theoretical & Applied Information Technology, 71(2).

Parent, M., & Reich, B. H. (2009). Governing information technology risk. California management review, 51(3), 134-152.

Phesa, M. (2021). Impression management observation in chairman statements in JSE Top 40 listed companies. (Masters Dissertation, University of Kwazulu-Natal).

Pholohane, M., Ajuwon, O., & Wesson, N. (2020). The Impact Of Shares Moving In And Out Of Ftse/Jse Top 40 Index. Journal of Smart Economic Growth, 5(2), 59-93.

Pirta, R., & Strazdina, R. (2012). Assessing the need of information technology control environment establishment. Information Technology and Management Science, 15(1), 99-104.

Prasad, B. D. (2008). Content analysis. Research methods for social work, 5, 1-20.

Raemaekers, K., & Maroun, W. (2014). Trends in risk-disclosure practices of South African listed companies University of the Witwatersrand, Faculty of Commerce, Law and Management …]. (Masters Dissertation, University of the Witswatersrand).

Rama, A. K., & Gunawan, E. (2020). Evaluation of IT Governance Implementation using COBIT 5 Framework and ISO 38500 at Telecommunication Industries. 2020 International Conference on Information Management and Technology (ICIMTech),

Ramamoorti, S., & Weidenmier, M. L. (2004). The pervasive impact of information technology on internal auditing.

Roberts, L., van Zijl, W., & Cerbone, D. (2020). The Integrated Reporting Committee of South Africa: On the balance of integrated reporting. In The Routledge Handbook of Integrated Reporting (pp. 37-66). Routledge.

Rossouw, G. J. (2005). Business ethics and corporate governance: A global survey. Business & Society, 44(1), 32-39.

Rubino, M., Vitolla, F., & Garzoni, A. (2017). The impact of an IT governance framework on the internal control environment. Records Management Journal., 27(1), 19-41.

Russell, F. (2010). FTSE/JSE Top 40 Index. Technology, 2(511,411), 7.81.

Salkind, N., & Van Zyl, L. (2014). Research methodology for the economic and management sciences. In: New Jersey: Pearson Publications.

Saunders, M., Lewis, P., & Thornhill, A. (2009). Research methods for business students. Pearson education.
Schutte, B., & Marx, B. (2018). The role of information technology in the risk management of businesses in South Africa. Journal for New Generation Sciences, 16(2), 92-111.
Selig, G. J. (2018). IT governance—an integrated framework and roadmap: How to plan, deploy and sustain for competitive advantage. 2018 Portland International Conference on Management of Engineering and Technology (PICMET),
Sityata, I. (2020). Risk management practices, disclosures and risk governance maturity of South African universities: an annual report disclosures analysis Cape Peninsula University of Technology]. (Masters Dissertation)
Sityata, I., Botha, L., & Dubihlela, J. (2021). Risk management practices by South African Universities: an annual report disclosure analysis. Journal of Risk and Financial Management, 14(5), 195.
Standardization, I. O. f. (2008). Corporate Governance of Information Technology. ISO/IEC.
Stults, G. (2004). An Overview of Sarbanes-Oxley for the Information Security Professional.
Surty, M., Yasseen, Y., & Padia, N. (2018). Trends in integrated reporting: a state-owned company analysis. Southern African Business Review, 22(1).
Tohidi, H. (2011). The Role of Risk Management in IT systems of organizations. Procedia Computer Science, 3, 881-887.
VAN VUUREN, H. J. (2006). DISCLOSING RISK MANAGEMENT POLICIES IN FINANCIAL STATEMENTS.
van Vuuren, H. J. (2016). RISK MANAGEMENT DISCLOSURE PRACTICES IN ACCORDANCE WITH KING II AND III: THE CASE OF SELECTED JSE LISTED COMPANIES. International journal of economics and finance studies, 8(2), 159-174.
van Vuuren, H. J. (2020). The Disclosure of Corporate Governance: a Tick-Box Exercise or Not? International Journal of Business and Management Studies, 12(1), 50-65.
van Zijl, W., & Hewlett, V. (2022). An analysis of the extent and use of fair value by JSE Top 40 companies. South African Journal of Accounting Research, 36(2), 81-104.
Viljoen, C., Bruwer, B., & Enslin, Z. (2016). Determinants of enhanced risk disclosure of JSE Top 40 Companies: the board risk committee composition, frequency of meetings and the chief risk officer. Southern African Business Review, 20(1), 208-312.
Wei-hua, X. (2011). The precaution of enterprise internal control under the ERP system. 2011 International Conference on Business Computing and Global Informatization,
Willows, G., & van der Linde, M. (2016). Women representation on boards: A South African perspective. Meditari Accountancy Research, 24(2), 211-225.
Wilson, J. (2014a). Essentials of business research: A guide to doing your research project. Sage.
Wilson, J. (2014b). Essentials of business research: A guide to doing your research project. Essentials of Business Research, 1-376.
Zhen, J., Xie, Z., & Dong, K. (2021). Impact of IT governance mechanisms on organizational agility and the role of top management support and IT ambidexterity. International Journal of Accounting Information Systems, 40, 100501.
.

7. APPENDIX A

IT GOVERNANCE AND RISK MANAGEMENT DISCLOSURE TESTS PERFORMED ON THE JSE TOP 40 LISTED COMPANIES

The results on the disclosure and King IV application test are presented in Table 2 and 3 below clearly indicating the total number of companies which complied and partly complied with the disclosure requirements.

Table 7.1: IT governance and risk management disclosures

			DISCLOSURE		
No	**Category**	**King IV Recommended Practices (IODSA, 2016)**	**Yes**	**No**	**Obscurely**
1	**IT Governance**	The board of directors should be responsible for the governance of IT by setting the direction on how IT should be addressed in a company.	39 Companies	0	1 Company
2	**IT Governance**	The board of directors should approve policy which articulates and gives effect to the set direction on the employment of IT.	38 Companies	0	2 Companies
3	**IT Governance**	The board of directors should delegate to management the responsibility to implement and executive an IT governance framework.	39 Companies	0	1 Company
4	**IT Governance**	The board of directors should ensure that IT is aligned with the performance and sustainability objectives of the company.	37 Companies	0	3 Companies
5	**IT Governance**	The board of directors should exercise an ongoing oversight of IT management to ensure alignment and integration of IT risks into organisation-wide risk management.	38 Companies	0	2 Companies
6	**IT Governance**	The board of directors should exercise an ongoing oversight of IT management to ensure proactive monitoring of intelligence to identify and respond to incidents, including cyber-attack risks, and adverse social media risks.	38 Companies	0	2 Companies
7	**IT Governance**	The board of directors should exercise an ongoing oversight of IT management to ensure management of the performance of,	33 Companies	0	7 Companies

		and the risks pertaining to, third-party outsourced services.			
8	**IT Governance**	The board of directors should monitor and evaluate significant IT investments and expenditure.	36 Companies	0	4 Companies
9	**IT Governance**	The board of directors should exercise an ongoing oversight of IT management to ensure ethical and responsible use of IT and compliance with relevant laws and standards.	38 Companies	0	2 Companies
10	**IT Governance**	The board of directors should exercise an ongoing oversight of the management of IT to ensure that IT systems supports confidentiality, integrity and availability of information.	38 Companies	0	2 Companies
11	**IT Governance**	The board of directors should exercise an ongoing oversight of the management of IT to ensure protection of privacy of personal information, security of information and protection of IT assets.	39 Companies	0	1 Company
12	**IT Governance**	The board of directors should ensure disclosure of an overview of its governance and management of IT.	36 Companies	0	4 Companies
13	**IT Governance**	The board of directors should ensure disclosure of key areas including objectives, significant changes in policy, risks including major incidents and significant risks exposed due to IT application systems.	37 Companies	0	3 Companies
14	**IT Governance**	The board of directors should ensure disclosure of actions taken to monitor the effectiveness of IT management and governance and how the outcomes were addressed.	36 Companies	0	4 Companies
15	**Risk Governance & Management**	The board of directors should assume the responsibility to govern risk or through a dedicated committee by setting direction for how risks should be approached and addressed in the organisation including the following the potential positive and negative effects of the risks in achievement of objectives.	39 Companies	0	1 Company

16	**Risk Governance & Management**	The board of directors should treat risks as an integral to the way it makes decisions and execute its duties as well as to approve policies which articulates and gives effect to its set direction on risks.	38 Companies	0	2 Companies
17	**Risk Governance & Management**	The board of directors should delegate to management the responsibility to implement and execute effective risk management and governance.	39 Companies	0	1 Company
18	**Risk Governance & Management**	The board of directors should evaluate and agree on the nature and extent of the risks that an organisation is willing to take in pursuit of its strategic objectives which includes limiting potential loss to the organisation due to IT risks and approving the organisation's risk appetite.	38 Companies	0	2 Companies
19	**Risk Governance & Management**	The board of directors should consider allocating the oversight role of risk governance to a dedicated committee which is the audit and risk committee.	39 Companies	0	1 Company
20	**Risk Governance & Management**	The board of directors should exercise ongoing oversight of risk management to ensure the following: i. Assessment of risks ii. Assessment of opportunities presented by risks iii. The integration and embedding of risk management in the business activities and culture of the organisation.	38 Companies	0	2 Companies
21	**Risk Governance & Management**	The board of directors should ensure the disclosure of nature and extent of the risks and an overview of the arrangements for governance and managing risk.	39 Companies	0	1 Company
22	**Risk Governance & Management**	The board of directors should ensure the disclosure of the key risks that the organisation faces, as well as undue, unexpected or unusual risks as well as the actions taken to monitor the effectiveness of risk management and how the outcomes were addressed.	39 Companies	0	1 Company

Table 7.2: IT risk governance and management King IV Application

			King IV APPLICATION		
No	**Category**	**King IV Recommended Practices (IODSA, 2016)**	**Yes**	**No**	**Partial**
1	**IT Governance**	The board of directors should be responsible for the governance of IT by setting the direction on how IT should be addressed in a company.	39 Companies	0	1 Company
2	**IT Governance**	The board of directors should approve policy which articulates and gives effect to the set direction on the employment of IT.	38 Companies	0	2 Companies
3	**IT Governance**	The board of directors should delegate to management the responsibility to implement and executive an IT governance framework.	39 Companies	0	1 Company
4	**IT Governance**	The board of directors should ensure that IT is aligned with the performance and sustainability objectives of the company.	37 Companies	0	3 Companies
5	**IT Governance**	The board of directors should exercise an ongoing oversight of IT management to ensure alignment and integration of IT risks into organisation-wide risk management.	38 Companies	0	2 Companies
6	**IT Governance**	The board of directors should exercise an ongoing oversight of IT management to ensure proactive monitoring of intelligence to identify and respond to incidents, including cyber-attack risks, and adverse social media risks.	38 Companies	0	2 Companies
7	**IT Governance**	The board of directors should exercise an ongoing oversight of IT management to ensure management of the performance of, and the risks pertaining to, third-party outsourced services.	33 Companies	0	7 Companies
8	**IT Governance**	The board of directors should monitor and evaluate significant IT investments and expenditure.	36 Companies	0	4 Companies
9	**IT Governance**	The board of directors should exercise an ongoing oversight of IT management to ensure ethical and responsible use of IT and compliance with relevant laws and standards.	38 Companies	0	2 Companies

10	**IT Governance**	The board of directors should exercise an ongoing oversight of the management of IT to ensure that IT systems supports confidentiality, integrity and availability of information.	38 Companies	0	2 Companies
11	**IT Governance**	The board of directors should exercise an ongoing oversight of the management of IT to ensure protection of privacy of personal information, security of information and protection of IT assets.	39 Companies	0	1 Company
12	**IT Governance**	The board of directors should ensure disclosure of an overview of its governance and management of IT.	36 Companies	0	4 Companies
13	**IT Governance**	The board of directors should ensure disclosure of key areas including objectives, significant changes in policy, risks including major incidents and significant risks exposed due to IT application systems.	37 Companies	0	3 Companies
14	**IT Governance**	The board of directors should ensure disclosure of actions taken to monitor the effectiveness of IT management and governance and how the outcomes were addressed.	36 Companies	0	4 Companies
15	**Risk Governance & Management**	The board of directors should assume the responsibility to govern risk or through a dedicated committee by setting direction for how risks should be approached and addressed in the organisation including the following the potential positive and negative effects of the risks in achievement of objectives.	39 Companies	0	1 Company
16	**Risk Governance & Management**	The board of directors should treat risks as an integral to the way it makes decisions and execute its duties as well as to approve policies which articulates and gives effect to its set direction on risks.	38 Companies	0	2 Companies
17	**Risk Governance & Management**	The board of directors should delegate to management the responsibility to implement and execute effective risk management and governance.	39 Companies	0	1 Company
18	**Risk Governance & Management**	The board of directors should evaluate and agree on the nature and extent of the risks that an organisation is willing to take in pursuit of its strategic objectives which includes limiting	38 Companies	0	2 Companies

		potential loss to the organisation due to IT risks and approving the organisation's risk appetite.			
19	**Risk Governance & Management**	The board of directors should consider allocating the oversight role of risk governance to a dedicated committee which is the audit and risk committee.	39 Companies	0	1 Company
20	**Risk Governance & Management**	The board of directors should exercise ongoing oversight of risk management to ensure the following: i. Assessment of risks ii. Assessment of opportunities presented by risks iii. The integration and embedding of risk management in the business activities and culture of the organisation.	38 Companies	0	2 Companies
21	**Risk Governance & Management**	The board of directors should ensure the disclosure of nature and extent of the risks and an overview of the arrangements for governance and managing risk.	39 Companies	0	1 Company
22	**Risk Governance & Management**	The board of directors should ensure the disclosure of the key risks that the organisation faces, as well as undue, unexpected, or unusual risks as well as the actions taken to monitor the effectiveness of risk management and how the outcomes were addressed.	39 Companies	0	1 Company

Fully Compliant Companies	**32**
Partially Compliant Companies	**8**
Non-Compliant Companies	**0**

8. Ethical Clearance

26 Aug 2022

Mr Taurayi Stephen Nyagope (221120330)
School Of Acc Economics&Fin
Westville

Dear Mr Taurayi Stephen Nyagope,

Original application number: 00018209
Project title: An analysis of information technology risks and governance disclosure: Evidence of the top 40 JSE listed companies.

Exemption from Ethics Review

In response to your application received on 19 Aug 2022 , your school has indicated that the protocol has been granted **EXEMPTION FROM ETHICS REVIEW.**

Any alteration/s to the exempted research protocol, e.g., Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through an amendment/modification prior to its implementation. The original exemption number must be cited.

For any changes that could result in potential risk, an ethics application including the proposed amendments must be submitted to the relevant UKZN Research Ethics Committee. The original exemption number must be cited.

In case you have further queries, please quote the above reference number.

PLEASE NOTE:
Research data should be securely stored in the discipline/department for a period of 5 years.

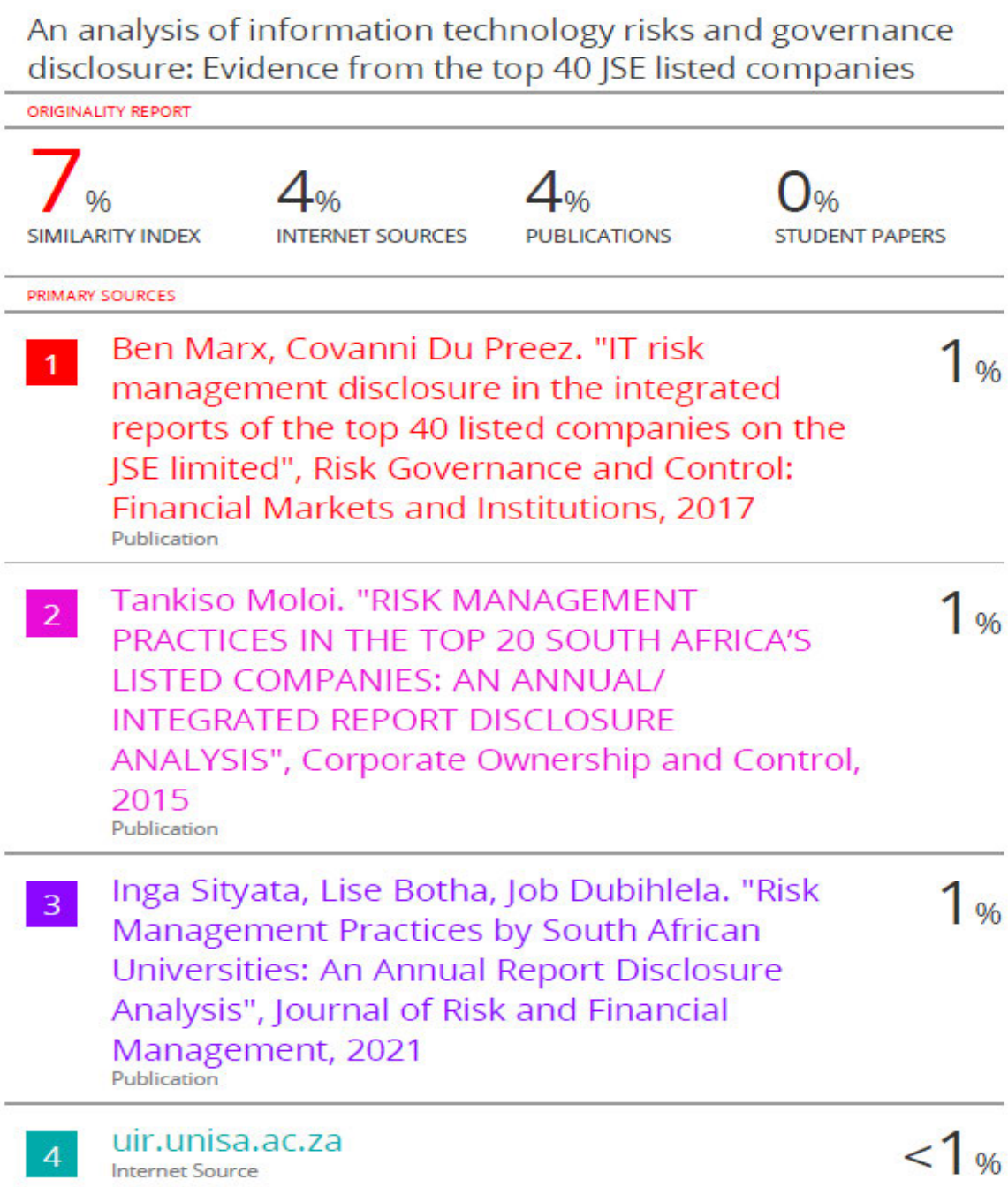
I take this opportunity of wishing you everything of the best with your study.

Yours sincerely,

[redacted]

Prof Josue Mbonigaba
Academic Leader Research
School Of Acc Economics&Fin

9. Turnitin Report



An analysis of information technology risks and governance disclosure: Evidence from the top 40 JSE listed companies

ORIGINALITY REPORT

7%	4%	4%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Ben Marx, Covanni Du Preez. "IT risk management disclosure in the integrated reports of the top 40 listed companies on the JSE limited", Risk Governance and Control: Financial Markets and Institutions, 2017 Publication	1%
2	Tankiso Moloi. "RISK MANAGEMENT PRACTICES IN THE TOP 20 SOUTH AFRICA'S LISTED COMPANIES: AN ANNUAL/ INTEGRATED REPORT DISCLOSURE ANALYSIS", Corporate Ownership and Control, 2015 Publication	1%
3	Inga Sityata, Lise Botha, Job Dubihlela. "Risk Management Practices by South African Universities: An Annual Report Disclosure Analysis", Journal of Risk and Financial Management, 2021 Publication	1%
4	uir.unisa.ac.za Internet Source	<1%