Analysing Information Technology Governance
Disclosure of the Top 40 JSE Listed Companies

MELINDA NGWENYA
22756132

Dissertation submitted in fulfilment of the requirements for the degree

*Magister Commercii*

in

*Accountancy*

at the

Vaal Triangle Campus

of the

North-West University

Supervisor: AM Moolman
Co-supervisor: Prof JP Fouché

November 2015
DECLARATION

I, Melinda Ngwenya declare that “Analysing Information Technology Governance Disclosure of the Top 40 JSE Listed Companies” is my own work; that all sources used or quoted have been indicated and acknowledged by means of complete references, and that this dissertation was not previously submitted by myself or any other person for degree purposes at this or any other university.

Signature: ________________________________

Date: ________________________________
ACKNOWLEDGEMENTS

First and foremost I want to thank my God for the gift of life, strength and guidance throughout the journey of my studies and this dissertation, without Him I would not have gotten this far.

I am very thankful to my supervisor, Mrs Anneke Moolman, for believing in me, her guidance throughout the study, her endless support and words of encouragement that kept me going even though I felt like giving up. I want to thank my co-supervisor, Prof Jaco Fouché, who also contributed towards this dissertation and for the guidance and support he gave me. I also want to thank the NWU Vaal Triangle Campus for the bursary opportunity, without the funds this study would not have been possible.

I want to thank my mother and brother for their moral support, love, motivation and for always believing in me. Through all the challenges and difficulties that I faced they were there to support and give me strength to always aim for success. I want to thank Brighton Dube, for his support, proofreading my dissertation and the love.

Lastly, I want to thank all my friends, for understanding and their moral support, especially Zanele Sobopha, for all her help and the motivation throughout the study.
ABSTRACT

Information Technology (IT) forms part of risk governance in accordance with King III, which assists in identifying and addressing IT-related risks. Identifying and addressing IT-related risks has become more important than ever in today’s competitive market environment. IT is a fast-developing industry that is continually subjected to significant changes and renewal. These continuous changes cause risks that have implications on the nature and effectiveness of both internal and external controls, which in turn impacts auditing. Specific and effective controls are therefore needed to mitigate the risks.

The nature and extent of the risks of internal controls vary depending on the characteristics and nature of the information system used by the entity. Entities are faced with different IT-related risks therefore IT-related risks are governed differently. Even though these IT-related risks are governed differently, IT still forms an integral part of the company’s risk management. Countries have different regulations that regulates IT governance disclosures; the King III report, as well as international regulations such as International Organisation for Standardisation (ISO’s), Sarbanes-Oxley Act (SOX) and International Standards on Auditing (ISA 315).

There appears to be a lack of guidelines that clarify the IT-related risks, and the extent thereof, that need to be disclosed in accordance with King III. Currently, the top 40 JSE listed companies are not fully compliant with the IT governance disclosure as required by King III. This study discusses the IT governance and disclosure requirements set out by the King III report and compares these requirements with the international requirements set out by the ISO’S, SOX and ISA 315.

The empirical review was conducted to determine to what extent the top 40 JSE listed companies comply with the IT risk governance disclosure in accordance with the King III report. The results were obtained by reviewing the, online published, top 40 JSE listed companies’ annual reports. The top 40 JSE listed companies were used as the basis of the study as these companies are required to comply with King III’s requirements.
The results that were obtained from the empirical review revealed that most top 40 JSE listed companies do not comply with the IT governance requirements of King III report.

The differences between King III, ISO’s, SOX and ISA 315 were determined by means of comparison. This was done in an attempt to clarify the IT governance disclosure of King III. The results led to recommendations made to King III in order to promote improved adherence for all South African companies.

**Keywords**: Information Technology (IT), IT-related risks, IT risk disclosure requirements, IT governance, JSE listed, King III
# TABLE OF CONTENTS

DECLARATION..............................................................................................................ii  
ACKNOWLEDGEMENTS ...............................................................................................iii  
ABSTRACT .....................................................................................................................iv  
TABLE OF CONTENTS .................................................................................................vi  
LIST OF TABLES ............................................................................................................x  
LIST OF GRAPHS AND FIGURES ................................................................................xi  
LIST OF ABBREVIATIONS ..............................................................................................xii  

CHAPTER 1 INTRODUCTION AND BACKGROUND TO THE STUDY ...........1  
1.1 BACKGROUND TO THE STUDY .........................................................................1  
1.1.1 The importance of IT in companies .................................................................2  
1.1.2 The risks of IT ..................................................................................................4  
1.1.3 The importance of IT governance and disclosure .............................................4  
1.1.4 Comprehensive summary and conclusion .......................................................7  
1.2 PROBLEM STATEMENT .......................................................................................8  
1.3 OBJECTIVES OF THE STUDY ...........................................................................8  
1.3.1 Primary Objectives ..........................................................................................9  
1.3.2 Secondary Objectives .....................................................................................9  
1.4 RESEARCH DESIGN AND METHODOLOGY ...............................................9  
1.4.1 Literature Review ............................................................................................10  
1.4.2 Empirical Study ...............................................................................................10  
1.4.3 Target Population ............................................................................................10  
1.4.4 Measuring instrument and data collection method .........................................11  
1.5 ETHICAL CONSIDERATIONS ..........................................................................11  
1.5.1 Chapter layout .................................................................................................12
CHAPTER 2 LITERATURE REVIEW ......................................................... 14
2.1 INTRODUCTION .................................................................................. 14
2.2 HISTORY OF IT .................................................................................. 14
2.3 RISK .................................................................................................. 15
2.3.1 IT-related Risks ............................................................................. 17
2.4 IT GOVERNANCE ................................................................................ 19
2.5 GOVERNANCE REGULATIONS SURROUNDING IT ................. 24
2.5.1 King III requirements for IT governance and disclosure ........ 28
2.5.2 SOX requirements for IT governance and disclosure .......... 30
2.5.3 ISA 315 requirements for IT governance and disclosure ..... 32
2.5.4 ISO requirements for IT governance and disclosure .......... 33
2.6 COMPARISON OF THE KING III WITH THE INTERNATIONAL REGULATIONS WITH REGARD TO IT GOVERNANCE AND DISCLOSURE ................................................................. 34
2.7 COMPREHENSIVE SUMMARY AND CONCLUSION ............... 39

CHAPTER 3 RESEARCH METHODOLOGY ........................................... 41
3.1 INTRODUCTION .................................................................................. 41
3.2 RESEARCH DESIGN .......................................................................... 42
3.2.1 Research Paradigms ..................................................................... 44
3.3 RESEARCH METHODOLOGY ............................................................. 44
3.4 VALIDITY AND RELIABILITY ............................................................... 47
3.5 DATA COLLECTION METHODS ............................................................. 49
3.5.1 Population ...................................................................................... 49
3.5.2 Sample ........................................................................................... 49
3.6 ETHICAL CONSIDERATIONS ............................................................... 51
3.7 DATA ANALYSIS ................................................................................. 51
CHAPTER 4 DATA ANALYSIS AND FINDINGS ........................................... 55

4.1 INTRODUCTION .................................................................................. 55

4.2 RECOMMENDED IT GOVERNANCE AND DISCLOSURE REQUIREMENTS ................................................................. 55

4.3 RECOMMENDED IT GOVERNANCE RISK DISCLOSURE REQUIREMENTS FOR THE PURPOSE OF TESTING ........... 56

4.4 RESEARCH FINDINGS OF COMPLIANCE WITH IT GOVERNANCE AND DISCLOSURE .................................................. 58

4.4.1 The Board of Directors should be responsible for IT governance ............................................................................... 58

4.4.2 IT should be aligned with the performance and sustainability objectives of the company ............................................. 59

4.4.3 The Board of Directors should delegate to management the responsibility to implement an IT governance framework ................................................................. 61

4.4.4 The Board of Directors should monitor and evaluate significant IT investments and expenditure .............................. 62

4.4.5 IT should form an integral part of the company’s risk management ............................................................................. 64

4.4.6 The Board of Directors should ensure that information assets are managed effectively ................................................. 65

4.4.7 A risk committee and audit committee should assist the Board of Directors in carrying out its IT responsibilities ........ 66

4.4.8 Total compliance of the evaluated companies ................................................................................................................ 68

4.5 COMPREHENSIVE SUMMARY AND CONCLUSION ...................... 69

CHAPTER 5 SUMMARY, CONCLUSION AND RECOMMENDATIONS ...... 70

5.1 INTRODUCTION .................................................................................. 70
LIST OF TABLES

Table 2.1: Comparison of the regulations .......................................................... 35

Table 3.1: A comparison between the qualitative and the quantitative approach ................................................................. 46

Table 4.1: Recommended IT governance risk disclosure requirements for the purpose of testing .................................................. 57
LIST OF GRAPHS AND FIGURES

Figure 2.1: Risk mitigation strategy .................................................................16

Figure 2.2: Summary of COBIT principles ......................................................23

Graph 4.1: Results of the requirement stating that the Board of Directors should be responsible for IT governance ........................................59

Graph 4.2: Results of the requirement stating that IT should be aligned with the performance and sustainability objectives of the company ..60

Graph 4.3: Results of the requirement stating that the Board of Directors should delegate to management the responsibility to implement an IT governance framework .....................................................62

Graph 4.4: Results of the requirement stating that the Board of Directors should monitor and evaluate significant IT investments and expenditure .................................................................63

Graph 4.5: Results of the requirement stating that it should form an integral part of the company's risk management ............................................65

Graph 4.6 Results of the requirement stating that the Board of Directors should ensure that information assets are managed effectively 66

Graph 4.7: Results of the requirement stating that a risk committee and audit committee should assist the Board of Directors in carrying out its it responsibilities .................................................................67

Graph 4.8: Results of the compliance of IT governance requirements ...........68
# LIST OF ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAATs</td>
<td>Computer Assisted Audit Techniques</td>
</tr>
<tr>
<td>CAE</td>
<td>Chief Audit Executive</td>
</tr>
<tr>
<td>CEO</td>
<td>Chief Executive Officer</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>COBIT</td>
<td>Control Objectives for Information Technology and Related Technology</td>
</tr>
<tr>
<td>EDP</td>
<td>Electronic Data Processing</td>
</tr>
<tr>
<td>IIA</td>
<td>Institute of Internal Auditors</td>
</tr>
<tr>
<td>IS</td>
<td>Information Systems</td>
</tr>
<tr>
<td>ISA 315</td>
<td>International Standards on Auditing</td>
</tr>
<tr>
<td>ISACA</td>
<td>Information Systems Audit and Control Association</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organisation for Standardisation</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITIL</td>
<td>Information Technology Infrastructure Library</td>
</tr>
<tr>
<td>JSE</td>
<td>Johannesburg Stock Exchange</td>
</tr>
<tr>
<td>SAICA</td>
<td>South African Institute of Chartered Accountants</td>
</tr>
<tr>
<td>SOX</td>
<td>Sarbanes-Oxley Act</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>USA</td>
<td>United States of America</td>
</tr>
</tbody>
</table>
CHAPTER 1
INTRODUCTION AND BACKGROUND TO THE STUDY

1.1 BACKGROUND TO THE STUDY

An organisation’s risk governance system is inclusive of both the process and people, but the internal control system forms the basis of governance (CLA, 2013:3). CLA (2013:3), accentuate that in order for the risk governance system to be effective it should be coupled with other monitoring and reporting systems. Information Technology (IT) forms part of risk governance in accordance with King III (SAICA, 2013), which assists in identifying and addressing IT-related risks. Therefore, IT is more important than ever in today’s competitive market environment. IT is defined as “the development, implementation, and maintenance of computer hardware and software systems to organise and communicate information electronically” (Dictionary.com, 2015:1). The use of IT plays an important role in various aspects of business by benefiting various elements of financial reporting on different levels and areas. For example, the application of electronic means for the purpose of internal control with the use of IT in the internal auditing field (Tiittanen, 2001, cited by Al-Refaee, 2013:110).

Marx et al. (2011:9-1) propose that IT is a fast-developing industry that is continually subjected to significant changes and renewal. Marx et al. (2011:9-1) further emphasise that data communications development leads to many transactions to be processed electronically. The developments have resulted in a shift in emphasis from central electronic data processing departments to end-user and distributed processing and this has brought about specific risks and control considerations. According to Hall (2011:36) the risks in the IT function has implications on the nature and effectiveness of internal controls, which in turn make an impact on auditing. Specific and effective controls are therefore needed to mitigate the risks.
Pirta and Strazdina (2012:98) claims the most essential tasks in the financial reporting processes are performed and supported by utilising IT. In order to ensure reliable financial reporting, more and more companies emphasise the use and development of effective IT controls in this dynamic environment (Pirta & Strazdina, 2012:99). However, the different processing methods used in IT have some significant issues (Ernst & Young, 2013:3). These issues include advanced technologies like cloud, social media and mobile devices. Ernst and Young (2013:3) further states that these issues seem to challenge the ability of companies to provide security to stakeholders who are already overwhelmed with rapidly expanding opportunities and pressures of shrinking margins.

It is evident that IT has revolutionised the scope and nature of worldwide communications, changing business processes and adapting the traditional boundaries of companies — internally between departments and externally with the stakeholders (Ramamoorti & Weidenmier, 2004:303). The importance of IT in companies is therefore becoming increasingly significant.

1.1.1 The importance of IT in companies

The unprecedented advances in technology have revolutionised nearly all aspects of life and sciences, including accounting. Today organisations are embracing the IT development to keep pace with growing competition in the market environment, improving productivity, helping companies improve business processes, achieve cost efficiencies and help drive revenue growth (Oven et al., 2012:5). IT has accelerated data processing and multiple tasks are achieved in a short period of time (Alkebsi et al., 2014:326). IT can convert raw data into useful information, convert processed information and use it as data in another processing step. It has also proved to be able to compile information into new, comprehensible, more attractive and more useful forms (Curtin et al., 1998:20). Processing is also fast and accurate with the use of IT even with large volumes of data.

Mackechnie (2015:1) identifies that IT has become the vital integral part of every business plan, from small businesses that own a single computer to
multi-national corporations that maintain mainframe systems and databases. IT plays an important role in companies since information is the lifeblood of modern business organisations; it is used to make decisions, convey needed actions, evaluate results, and exchange ideas (Curtin et al., 1998:238). Whittington and Pany (2006:271) points out that IT-based systems enhance the reliability of financial information and it processes transactions uniformly, eliminating human errors that may occur in a manual system. Therefore, IT plays an ever-growing role in how organisations achieve their business objectives (Hirth, 2008:16).

Moorthy et al. (2011:3523) indicate how technology, information systems (IS) and electronic data processing (EDP) have changed the way organisations conduct business. This has in turn promoted operational efficiency and aids decision-making, which contributes to an effective audit force, directing audit resources to the maximum benefit of the organisation (Moorthy et al., 2011:1). The internal control environment of automated IS and the use of these systems are addressed by IT audits (Decimiso, 2014:1 and Mizoguchi, 2012:13). In support of Moorthy’s statement, Amnseven (2010:1) states that, for management to improve the efficiency and effectiveness of their business process, work group collaboration and management decision-making, IT assistance is needed, thus helping managers strengthen the position of their companies in a rapidly changing environment.

A number of studies indicate that internal audit functions are focusing on technology as a way to improve productivity and the organisation’s risk management process. Such studies include a study by Neo (1988:191) that propose that an understanding of the potential processes of using IT in internal auditing may lead to a competitive advantage. Bierstaker et al. (2001:159) state that “advancement in IT improves the efficiency and effectiveness of internal audits”. Activities such as ongoing monitoring of certain internal controls can be automated by technology (Verver, 2009:1). However, IT, as well as the rapid change thereof, has brought forth risks that companies need to address and govern.
1.1.2 The risks of IT

Companies have become increasingly vulnerable to IT-related risks because of the evolvement of IT in central components of business operations (IBM, 2011:2). IT events can no longer be contained without affecting overall business functions (IBM, 2011:2). Ellingwood (2011:1) identify that as companies continue to automate tasks, the increase of IT usage leads to increased risks such as:

- The use of social media technologies that is expanding in which there are risks of failure to protect the company’s brand when employees divulge too much information to the public along with unauthorised access to confidential data and regulatory or legal violation.
- An increase in malware that may result in risks of loss or theft of critical business information, hardware impacts and risk of loss of productivity.
- The use of end-user computing applications that continues to evolve, which cause risks such as misstatement of financial statements.
- The risk of failure to comply with corporate IT policies and controls.
- The risk of compromised system or data breeches.
- The risk of recovery programs when computers fail such as failure to recover internal audits already performed.
- Uncontrolled access to data, leading to corruption, sabotage, manipulation and so on.
- Unauthorised changes of master files.

These risks affect organisations and its internal audit functions, making it important for the entity’s systems to address these risks and limit the risks through effective controls (Ellingwood, 2011:2 and Marx et al., 2011:9-12 and Mizoguchi, 2012:14), which forms part of IT risk governance.

1.1.3 The importance of IT governance and disclosure

The IT governance network (2013:1) defines IT governance as the “senior management’s ability to direct, measure and evaluate the use of an
enterprise's IT resources in support of the achievement of the organisation's strategic objectives. Leadership, organisational structure and processes are used to leverage IT resources to produce the information required and drive the alignment, delivery of value, management of risk, optimised use of resources, sustainability and the management of performance”.

IT governance arrangements expound the decisions, the participation by different stakeholders, and the structures, processes, responsibilities and other mechanisms required to make decisions (PWC, 2015:1). This includes ensuring the right capacity, processes and structures in order to make the right decisions in order to achieve alignment, manage risks, enable change, deliver quality IT services, and manage service costs (PWC, 2015:1). IT is no longer regarded as simply a mechanism for processing, but as a strategic resource, and for this reason, strategic management no longer focuses merely on risks and controls, but regard IT as a business project designed to meet business needs (Marx et al., 2011:9-16).

The King III report and international regulations such as the International Organisation for Standardisation (ISO’s), Sarbanes-Oxley Act (SOX) and International Standards on Auditing (ISA 315), regulates the IT governance disclosure. According to the ISA 315 paragraph 5, information systems, which consists of infrastructure (physical and hardware components), software, people, procedures and data including the related business processes are relevant to report and communicate in the annual reports because many IS’s make extensive use of IT (SAICA, 2015:315).

ISA 315 paragraph A66 indicates that the nature and extent of the risks of internal controls vary depending on the characteristics and nature of the IS used by the entity (SAICA, 2015:294). The responses to the risks arising from the use of IT should therefore be managed accordingly. Even though risks are governed according to the IT-related risk faced by the entity, IT should still form an integral part of the company’s risk management. Management should regularly demonstrate to the Board of Directors that the company has adequate business resilience arrangements in place for disaster recovery, which should also be disclosed in the annual reports (Roos, 2012:12).
The annual report is a significant document through which an organisation specifically provides information to its shareholders and its stakeholders, on every important aspect that affects the company’s business, performance, results and future prospects. Information on the company’s governance structures and practices are also of importance to shareholders, investors and other stakeholders (Marx, 2009:35). For this reason, ISA 315 paragraph A40 states that the international regulation requires companies to govern inconsistencies between the entity’s IT strategy and its business strategies, changes in the IT environment and installation of significant new IT systems that relate to financial reporting (SAICA, 2015:319). In Canada, and in most other countries, IT governance is a common topic at IT seminars and conferences (Brisebois et al., 2009:30). IT risk governance is therefore also extremely relevant on an international scale.

Brisebois et al. (2009:30) affirm that IT governance should be reviewed in terms of how it adds value to the company and it should conform to the overall corporate governance strategy of the organisation. King III was introduced in order to provide guidance on corporate governance for South African companies and stresses the importance of conducting business reporting in an integrated manner (IODSA, 2009:4). In accordance with IODSA (2009:17) King III deals with IT governance in detail as there is no doubt that there are operational risks when IT is used by companies, as confidential information may leave the company. Therefore IT governance should seek to provide confidentiality, integrity and availability of the functioning of the IS with assurance that the systems are useful.

Effective management of information and IT-related risks has become critical to organisations and in order to address these risks, organisations need to have appropriate strategies in place (GIAR, 2008:3). Research conducted by Janse van Vuuren (2006:172) on King II reports that the JSE listed companies were not complying with IT governance disclosures because the findings indicated that only 46% of companies disclosed in their annual reports that their risk management process attends to IT-related risks. King II was then replaced by the King III report. The King III sets forth the “apply or explain”
principle, which means that the Board of Directors should act in the best interest of the company and meet the corporate governance requirements (IODSA, 2009:3). Failure to do so would lead to an explanation to be provided as to why they do not comply with the requirements. Should companies therefore not be disclosing anything with regard to IT risk governance, the assumption is made that companies are not complying with the King III IT governance and disclosure requirements. Another assumption is made that if companies did not comply it is because the companies do not understand or misinterpret the governance and disclosure requirements.

IT is important to manage the transactions, information and knowledge necessary to initiate and sustain a company, but it is not clear whether the goal is achieved (Gowell & Anderson, 2012:4). This is the central finding of a survey of more than 500 Chief Audit Executives (CAEs) conducted by The Institute of Internal Auditors (IIA’s) Audit Executive Centre in March 2011. In this survey, 48% of the CAEs described their ability to use technology as inadequate, while only 14% rated the performance of their teams in this area to be above average (Gowell & Anderson, 2012:4). Organisations develop suitable internal controls, but the disclosure of the IT-related risks and the methods that companies use to overcome these risks are left unaddressed or partially addressed (Hirth, 2008:2). This results in an incomplete plan that may expose the organisation to great risks of data loss, material misstatements of financial statements or potential failure of the organisation (Hirth, 2008:2). It can therefore be concluded that there is a lack of experience, ability and knowledge with regard to the governance of IT.

1.1.4 Comprehensive summary and conclusion

The above discussions emphasised the significance and vital role IT plays in companies, but the current technological era introduces new risks to companies, which companies need to address and disclose in their annual reports. It can be concluded that the IT risk governance disclosure is essential for every company to help the users of the annual reports understand the risks that the company is exposed to and the methods that they can implement to address or minimise these risks. King III and international regulations clearly
indicate the importance of disclosure of IT-related risks and methods used to govern these risks, as this brings assurance to the users of companies’ annual reports on the abilities of the company and enable them to identify and formulate strategies to deal with IT-related risks.

1.2 PROBLEM STATEMENT

Given the risks that arise in an IT environment as discussed, the problem appears to be non-compliance of companies with the IT disclosure requirements due to lack of guidelines that clarifies the King III report IT governance and disclosure requirements. Current research does not address the IT governance disclosure requirements taking King III, ISO’s, SOX and ISA 315 into consideration. It is apparent that no studies have been made to evaluate the extent to which the companies comply with King III IT governance and disclosure requirements. A previous study included the evaluation of companies’ compliance with IT disclosure requirements based on the King II report (Janse van Vuuren, 2006:172). Currently there are indications that the top 40 JSE listed companies do not comply with the IT governance disclosure as required by King III. Therefore this study aims to evaluate to what extent the top 40 JSE listed companies comply with the IT governance and disclosure requirements as set by the King III report. This study also aims to clarify King III IT governance disclosure requirements to companies, through analysing the difference in IT governance disclosure between King III, ISO’s, SOX and ISA 315. This study aims to answer the following research question:

To what extent does the top 40 JSE listed companies comply with the King III IT governance disclosure requirements?

1.3 OBJECTIVES OF THE STUDY

The study addresses the following objectives:
1.3.1 Primary Objectives

In order to address the research question in Section 1.2, the study aims to evaluate the extent to which the top 40 JSE listed companies comply with the IT governance disclosure in accordance with King III and to review the difference between the King III report, ISO's, SOX and ISA 315 governance disclosure requirements.

1.3.2 Secondary Objectives

In order to achieve the primary objective, the following theoretical and empirical objectives are formulated for the study:

I. Determine current IT governance disclosure requirements according to King III.

II. Determine IT governance disclosure requirements according to the ISO’s, SOX and ISA 315.

III. Evaluate the top 40 JSE listed companies to identify the extent to which they comply with the King III IT governance and disclosure requirements.

IV. Make recommendations to King III IT governance disclosure requirements, in accordance with ISO’s, SOX and ISA 315 to clarify disclosure requirements to South African companies that have to comply with King III.

1.4 RESEARCH DESIGN AND METHODOLOGY

A quantitative research approach is followed in order to assess the companies that comply with the IT governance disclosure requirements in accordance with King III and international regulations.

Most of the secondary objectives of the study are achieved through a qualitative research approach whereby a literature review on previous studies regarding IT governance disclosure requirements was studied. A review of the King III report is also conducted, ISO’s, SOX and ISA 315 to gain an understanding of what the companies should disclose with regard to IT governance. A comparison is made between the King III IT governance
disclosure requirements, as well as that of ISO’s, SOX and ISA 315 in order to indicate the differences and to make recommendations to King III.

The top 40 JSE listed companies’ annual reports are reviewed in order to assess what IT-related risks these companies have as well as the methods used to manage the risks identified.

1.4.1 Literature Review

Secondary data sources include relevant textbooks, journal articles, newspaper articles and the Internet. A literature review forms a significant part of this study. The literature review is conducted in order to determine IT-related risks, the importance of disclosing IT-related risks and the standards followed by companies to govern and disclose IT-related risks. The literature review also assists with the comparison of King III, ISO’s, SOX and ISA 315 with regard to the IT governance disclosure.

1.4.2 Empirical Study

The empirical section of this study comprises the following methodology dimensions:

1.4.3 Target Population

The empirical study is based on the primary data regarding IT governance disclosure that are collected by reviewing the top 40 JSE listed companies’ annual reports, published online. The top 40 JSE listed companies were used as the basis of the study as these companies have to comply with King III requirements in terms of the listing requirements (JSE, 2012:6). These companies are the largest companies in South Africa and representative of the different industries of the country. As these are the top companies, smaller and growing companies aspire to the governance and disclosure of these top companies.

The empirical review is conducted to determine to what extent these companies comply with the IT risk governance disclosure in accordance with
the King III report. This is conducted in a way to aim to close the gap between King III, ISO’s, SOX and ISA 315.

The international regulations (ISO’s, SOX and ISA 315) used in this study are the regulations that are mostly used by the G8 countries (Canada, France, Germany, Italy, Japan Russia, United Kingdom (UK) and United States of America (USA) to deal with the countries’ IT governance disclosure (Coetzee et al., 2010:7). The G8 countries are the most powerful countries in the world which aim to solve global problems by coming up with action plans that will solve issues discussed in their annual meetings (BBC news, 2013:1). Therefore it is deemed fit to use the regulations that govern the most powerful countries in the world in order to make recommendations that will enhance the King III report.

1.4.4 Measuring instrument and data collection method

The top 40 JSE listed companies ranked by market capitalisation on the JSE’s All Share Index as of the 31st of March 2015 were chosen. The latest publicly available annual reports of the selected companies were used because the companies have different reporting periods, causing some companies’ 2014 and 2015 annual reports to be used, due to companies having six months after year-end to finalise their annual reports (National Treasury, 2012:10). The assumptions that were made in this study includes the assumption that if companies are not mentioning anything with regards to IT risk governance, the companies are not complying with the King III IT governance and disclosure requirements. The other assumption made is that if companies did not comply with the IT governance and disclosure requirements they either do not understand or misinterpret the requirement.

1.5 ETHICAL CONSIDERATIONS

All ethical concerns were considered by the author and the author is confident that no ethical issues may arise in the study as only publicly available sources were used and the company names were not mentioned in order to protect their identities.
1.5.1 Chapter layout

This study comprises the following chapters:

**Chapter 1 Introduction and background to the study**

Chapter 1 serves as an introduction that provides the background to the study. It also points out the problem statement, primary objective and the secondary objectives of the study. A brief layout of the methodology followed in this study is also given in this chapter.

**Chapter 2 Literature Review**

This chapter reviews the history of IT to gain a better understanding of the role of IT in accounting and auditing. The literature review also includes an overview of King III, ISO’s, SOX and ISA 315’s IT governance disclosure requirements. In addition, a comparison of IT governance disclosure between King III, ISO’s SOX and ISA 315 is made.

**Chapter 3 Research design and methodology**

Chapter 3 discusses the research methodology followed in this study. It gives an in depth description of different methodologies and gives reasons for choosing the methodology followed in this study.

**Chapter 4 Results and Findings**

The purpose of this chapter is to analyse and provide the results of the extent to which the annual reports of the top 40 JSE listed companies comply with the IT governance and disclosure requirements of King III.

**Chapter 5 Conclusions and Recommendations**

A summary of the study is provided in this chapter in the light of the objectives set out in Chapter 1. A summary and conclusion of the recommendations to King III are made in an effort to overcome the gap between South African and international IT governance disclosure requirements identified in Chapter 2. The recommendations that will be made to the King III will also improve the
understanding of IT governance and disclosure requirements to the top 40 JSE listed companies that are currently not meeting the requirements as found in Chapter 4.
CHAPTER 2
LITERATURE REVIEW

2.1 INTRODUCTION

IT is regarded as the most vital organisation function; it does not matter whether someone plans to be an entrepreneur and run their own business, or become a manager of a corporation, managing IT is a major responsibility (O’Brien, 1996:494). Its increased capabilities has offered organisations opportunities to be innovative and to exploit all technology resources to meet organisations' objectives in a more sophisticated and strategic way (Grant et al., 2010:103).

Even though the main aim of this study is to evaluate the extent to which companies comply with the IT governance disclosure in accordance with King III and to review the difference between the King III, ISO’s, SOX and ISA 315 IT governance disclosure requirements, it is necessary to have a brief understanding of the history of IT and the background of risks in general. It is also necessary to identify the risks caused by IT in companies as well as understand the extent of damage that these risks hold for companies.

2.2 HISTORY OF IT

Most technological changes took place since the 1950s, computers and the Internet were unknown functions before that period (Forest Service Centennial, 2011:6). Today the heart of modern IT is a computer (Curtin et al., 1998:22). Before there were computers, word processors and the Internet, companies used a number of tools such as pencils, paper and typewriters (Forest Service Centennial, 2011:7). After the development of computers and centralised computer centres, named data-processing stations, were created to replace traditional methods of accounting and record-keeping by a new industry of data processing that flowed in the organisation (Mahoney, 2011:4).
Slowly, new approaches of processing and storing information were introduced and information processing became both more flexible and more powerful (Curtin et al., 1998:240). The industrial revolution resulting in IT growth in business activities, led to wide-spread adoption of IT auditing (Byrnes et al., 2012:2). Historically, organisations were accustomed to manual audit procedures and the early components of IT auditing were drawn from several areas. First, traditional auditing contributed knowledge to the internal control practices and the overall control philosophy. Another contributor was IS management and IT governance, which provides methodologies necessary to achieve successful design and implementation of systems (Gallegos & Senft, 2012:3). The constant changes in IT introduced advanced automated audit procedures, which included the introduction of computer-assisted audit techniques (CAATs) that facilitate data extraction, sorting and analysis procedures (Byrnes et al., 2012:2).

The development of IT has changed and improved the business environment by shortening the data processing period and achieving multiple tasks (Alkebsi et al., 2014:325). According to Hall (2011:1) IT has inspired the re-engineering of traditional company methods that were used, to promote more efficient operations and provide methods to redesign and improve communication skills within the entity and between the entity’s customers and suppliers. However, the advances of IT have also introduced new risks that require unique and effective risk governance strategies by companies (Hall, 2011:1).

2.3 RISK

Risk is regarded as a general concept that is an everyday phenomenon in the business industry (Coetzee et al., 2010:18). Janse van Vuuren (2006:13) perceives risk as a negative perspective as it usually focuses on potential losses. The business world is ever-changing nowadays, its unpredictable volatility seems to become more complex each day, and therefore it is fraught with risks (PWC, 2008:3).
Risk can be defined in many different ways but the definition as stated by Coetzee et al. (2010:18) is appropriate for this study: “risk is the possibility that an accident or a loss could occur, or that there is a threat as a result of an uncertainty”.

A lot of managerial decisions are influenced or subjected to uncertain events to occur and therefore risk becomes an overriding factor (Wall, 2011:1). Risks should be identified, governed and monitored to avoid losses, thus the internal control engagements are now the focus area of every organisation (Coetzee et al., 2010:12). The main objective is to identify risks that threaten the organisation’s objectives before investigating the manner in which management addresses and manages these risks. A common risk mitigation strategy was formulated for any organisation to follow (Mar et al., 2012:12) and is set out in Figure 2.1.

**Figure 2.1: Risk mitigation strategy**

![Risk mitigation strategy diagram]

Source: Mar et al. (2012:12)

The first initial step is to identify and assess the risk, followed by measurement of the risk. After the risks are measured, it can then be classified according to the impact it has on the company.
The risk can either be accepted as a cost of conducting business, or eliminated by replacing the technology with a more effective one, or shared and mitigated by implementing controls to prevent the risk from manifesting again (Mar et al., 2012:12). The third step is to report and disclose the risk in the company's annual reports and lastly the company has to integrate the risk strategy with the strategies and business plans of the organisation. An understanding of the business risks the entity faces increases the likelihood of identifying risks of material misstatement in the financial statements (SAICA, 2013:31). IT-related risks could therefore also affect the decision-making process of the company’s management and stakeholders.

2.3.1 IT-related Risks

According to ISACA (2009:7) an IT-related risk can be defined as the business risk that is associated with “the use, ownership, operation, involvement, influence and adoption of IT within an entity”. It involves IT-related events that could potentially influence the business. It can occur with both uncertain frequency and magnitude, creating challenges in meeting strategic goals and objectives. Although IT can enhance the organisation’s productivity and effectiveness, it can also affect the company’s overall performance due to different risks affecting the processing methods used in an IT environment (Loebbecke et al., 2000:330). Most often IT-related risks are ignored compared to other business risks and as a result these risks lead to substantial losses (ISACA, 2009:3). The IT-related risks include the risks listed and defined below (Mar et al., 2012:11 and Marx et al., 2011:9-16):

- Unauthorised access: Access to the company’s master files by an unauthorised employee due to a lack of proper online restrictions such as user IDs and passwords. Unauthorised activities may be initiated through the computer resulting in improper changes in the software programs. Master files and confidential information of the company may be obtained.

- Loss of data: Most of the company’s important information is processed and stored on computers and it is centralised. When data are centralised or kept in one place, there is an increased risk of loss or destruction of all data files with severe ramifications. When the entire company system
experiences such destructions, the organisation usually incur serious business interruption and loss of income.

- Social networking: Social media technology is expanding to all business areas and companies are exposed to the risk of brand violation, regulatory and legal violation.

- Malware: A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or boost sector of the hard drive. When this replication succeeds, the affected areas are then said to be "infected". Computer viruses continue to increase at a rapid speed increasing the risks of loss of company information, loss or corruption of the company’s hardware and loss of production.

- Systematic versus random errors: Most organisations have replaced the manual procedures with the technological procedures to reduce the risks of human error. However, systematic errors have increased due to the uniformity of computer processing. Once the procedures are programmed in the computer software, the computer processes the information consistently for all transactions until the programmed procedures are changed. Therefore the risk of incorrect programming may exist, which will affect the reliability of computer processing and may result in many misstatements. This risk is usually not easily identified and may only be identified if the system is programmed to recognise unusual transactions when processed or when transaction audit trials are inadequate.

- IT governance: Failure to comply with corporate IT policies and controls, operational impacts, IS risks, regulatory violations, and duplication of efforts, increased costs and inefficiencies.

IT-related risks affect all organisations. The graph below, which is drawn from a survey conducted by the IBM security services in 2012, indicates in percentages how the IT-related risks are ranked by the respondents of the survey. Data breaches, data theft and cybercrime are the top IT-related risks that pose the greatest threat to the reputation of a company.
Graph 2.1: IT-related risks posing as the greatest threats to business reputation

<table>
<thead>
<tr>
<th>Risk</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology adoption (e.g. iCloud)</td>
<td>3%</td>
</tr>
<tr>
<td>Inadequate business continuity plans</td>
<td>8%</td>
</tr>
<tr>
<td>Website outages</td>
<td>14%</td>
</tr>
<tr>
<td>Data loss/failed backup restore</td>
<td>15%</td>
</tr>
<tr>
<td>Data breaches/data theft/cybercrime</td>
<td>17%</td>
</tr>
<tr>
<td>Data breaches/data theft/cybercrime</td>
<td>22%</td>
</tr>
<tr>
<td>Website outages</td>
<td>37%</td>
</tr>
<tr>
<td>Data loss/failed backup restore</td>
<td>44%</td>
</tr>
<tr>
<td>Technology adoption (e.g. iCloud)</td>
<td>61%</td>
</tr>
</tbody>
</table>

Source: Mar et al. (2012:3)

In terms of addressing the different IT-related risks associated with greater reliance on IT, companies often implement controls specific to the IT function (Loebbecke et al., 2000:332 and Marx et al., 2011:95 and Mizoguchi, 2012:4) in order to reduce failure and disappointment caused by inappropriate IT activity, and to improve the performance of IT. Effective IT governance needs to be implemented in an organisation, as IT-related risks can really affect the company’s activities negatively and the ever-changing IT environment needs proper and effective governance procedures (Guldentops, 2001:14).

2.4 IT GOVERNANCE

The use of IT poses various inherent risks that require governance and control to ensure the function supports the company’s strategic objectives. The importance of risk governance, which involves the identification of risks faced by business organisations and the implementation of the systems to mitigate these, has been recognised (Puttick & Van Esch, 2003:210). In 2004, Kordel conducted research that indicated that one of the key factors distinguishing and separating top performing companies from standard-performing companies is the level of involvement and leadership of management in making key IT decisions and the manner in which IT is supported by the entity (Butler et al., 2010:34). IT risk governance is referred to as the essential process to aid companies in implementing new business changes and, where
appropriate, invest in IS to accommodate these changes (Noraini et al., 2015:184). The development approach in changing the audit work to corporate governance is now based on IT because the auditor now uses the technological methods and systems (Pickett, 2011:230). The auditor now has to foresee IT-related risks, identify them and ensure the company manages and controls these risks across the organisation (Pickett, 2011:230). The IT audit function came into being because (Gallegos & Senft, 2012:1):

- Auditors realised that computers have influenced and affected their ability to perform the attestation function.
- Management of corporate and information processing realised that computers are now key resources for competing in the business environment, IT is similar to other valuable business tools within the entity used for competing and doing work effectively, and therefore the need for computer control and auditing became crucial.
- Professional bodies’ e.g Information Systems Audit and Control Association (ISACA), organisations and governance entities recognised the need for IT governance and auditability.

In accordance to ISACA (2009:2) risks play a critical role nowadays as almost every business decision requires those charged with governance to balance risk and governance. IT-related risks are most often overlooked. IT provides opportunity for development and growth but also presents threats such as disruption, deception and theft (Mar et al., 2012:3). IT governance was introduced to effectively manage and deal with the risks imposed by IT.

In order to minimise and control these risks successfully, IT risk assessment policies and strategies should be developed and implemented in organisations (Noraini et al., 2015:184). According to Mar et al. (2012:3) IT governance is essential to protect stakeholders, assets and the company’s confidential information, to demonstrate safe, efficient and ethical behaviour; preserving reputation, trust and the brand of an organisation. Mar et al. (2012:3) argues that IT governance should provide assurance and reliability, in which management plays a vital role in assuring the reliability of information
provided by the entity’s IT. The IT governance strategies provided by management should remain sufficient and effective in order to address the IT-related risks of the company.

IT governance is a very important issue at present as an integral component of any corporation or organisation because the most important IT issues for the near future in the private and public sector, are not technology-related, but governance-related (Guldentops, 2002:15). The purpose of IT governance is to direct IT endeavours to ensure that IT performance meets the objectives set out in an entity’s strategy (Noraini et al., 2015:18). It has been claimed that an organisation needs to provide an equivalent level of commitment to IT governance as it allocates to corporate governance in order to achieve corporate success (Rao, 2003:1).

IT governance focuses specifically on IT systems, its performance and risk management. The main objectives of IT governance are to assure that the investments in IT add business value and to eliminate or minimise the risks that are associated with IT (Brisebois et al., 2009:31). In an organisation, IT governance entails general responsibilities (University of Utah, 2015:1) which are as follows:

- Align IT with the strategic mission, direction and initiatives of the entity.
- Establish an overall IT funding model for total IT expenditures in the organisation.
- Establish the technical standards and company-wide infrastructure services to support the mission of the company.
- Govern the definition process and use of organisational data.
- Govern the degree of IT data related to risk.

IT governance has a framework namely control objectives for information technology and related technology (COBIT) that entities should follow, apart from the different acts and regulations applied by the different countries. COBIT is an IT governance framework or set of best practices for IT governance. Steenkamp (2009:10) determined in a research study that
COBIT was singled out to be the only available IT governance framework. COBIT was established by the IT governance Institute and the ISACA. It was published in 1996 to serve as a framework that provides a common language for business executives to communicate each other’s goals, objectives and results (ISACA, 2012:1). The motivations to why COBIT was singled out as the only available IT governance framework (Steenkamp, 2009:10) are as follows:

- It is stated in King III as one of the possible IT governance frameworks to apply in order to achieve IT governance.
- It is a comprehensive framework, covering all the important elements of IT governance, rather than focusing on a specific part of it, as ISO 17799 and Information Technology Infrastructure Library (ITIL) do.
- COBIT is business-orientated.
- It is accepted all across the world (internationally recognised).
- It is available for free.
- It incorporates the inputs of the experts in terms of IT.
- It can be used by any organisation towards IT governance because it can be adapted to the size, level of IT usage, complexity and needs of each organisation.
- COBIT is often used by managers and auditors to assess an entity’s system of IT internal control for compliance with SOX.

COBIT was chosen, for these reasons, as the only framework that can guide other acts and regulations to have similar requirements as it was established for different countries. It is important to have an understanding of what an ideal act or regulation should comprise and this can be determined by analysing the structure of the COBIT framework.

IT governance is a part of organisation governance and COBIT helps companies to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource usage (ISACA, 2012:5). COBIT has principles that are adaptive to any organisation of any
size, whether public, non-profit organisation or profit-making organisation and these principles are summarised in Figure 2.2 (ISACA, 2012:6).

**Figure 2.2: Summary of COBIT principles**

![COBIT 5 principles diagram]

Source: ISACA (2012:8)

In accordance with ISACA (2012:10), COBIT combines the five principles that allow the organisation to build effective and efficient IT governance. The first principle states that the IT governance should meet stakeholders’ needs and that means that the organisation should consider all stakeholders when establishing the governance techniques. The techniques should benefit both the company and its stakeholders. The resource utilised for risk-assessment decisions should not affect the stakeholders’ integrity or investment decisions. The second principle states that the IT governance framework should cover the organisation from end to end and this means that the organisation should integrate governance of company IT into corporate governance, in other words, the governance system for the company IT proposed by COBIT 5, integrates seamlessly in any governance system because COBIT 5 aligns with the latest views on governance. The third principle points out that it should apply a single integrated framework and this simply means that COBIT 5 has all the latest regulations integrated.
The fourth principle states that the framework should enable a holistic approach, meaning factors that, individually and collectively, influence the organisation's IT should be effectively governed and managed. Lastly, the principle states that the framework should separate governance from management and it means that governance is the responsibility of the Board of Directors under the leadership of the chairperson while management has the responsibility of the executive management under the leadership of the Chief Executive Officer (CEO) (ISACA, 2012:40).

After COBIT was established, different countries also established their regulations and acts that deal with IT governance. Examples of this are King III that governs South African companies, SOX that governs the USA and four of the G8 countries, ISO’s that is an independent non-governmental standard and the ISA 315 that governs South Africa as well as the G8 countries. Steenkamp (2009:18) is of the opinion that the requirements in King III relating to IT governance and the processes of COBIT are well aligned, and, as a result, King III can be used to create an internal IT governance framework for an entity.

SOX is also aligned with COBIT because COBIT is often used by managers and auditors to assess an entity’s system of IT internal control for compliance with SOX (Steenkamp, 2009:10). IT governance is regulated by these regulations. An in-depth description of IT governance regulations follows below.

**2.5 GOVERNANCE REGULATIONS SURROUNDING IT**

IT regulations provide the legal framework for collecting, storing, disseminating electronic information in the global marketplace and the governance of IT (HG.org, 2012:1). Recently there has been a common increase in the number of systems affecting the usage of IT and also the number of circumstances where legal actions need to be considered. This is due to the need to safeguard against a wide range of new IT-related risks and from a common increase in corporate regulations (National Computing Centre, 2005:53). ISACA (2012:36) reasons that the heart of most regulations
is the intention of protecting the confidentiality, integrity, and availability of information that influence an organisation’s stakeholders.

Most regulations have the same intentions (protecting the confidentiality, integrity, and availability of information that influence an organisation’s stakeholders), because of various factors affecting IT. Some of the contributing factors are (National Computing Centre, 2005:54):

- A greater interest by regulators in the operations of all organisations caused by major corporate financial failures and scandals, which resulted in regulations like the USA SOX forcing Board of Directors to express opinions about their systems of control.
- Concerns about security and privacy influenced by the overall increase in use of computers and networks and the impact of the Internet.
- Laws to protect personal information and its potential misuse in electronic form.
- A growth in the use of computer systems and networks for criminal activity and terrorism, including viruses, hacking and money laundering.
- A growth in complex contractual relationships between IT services and products (outsourcing, managed services, product licenses).
- The growth in all forms of electronic media and the potential for misuse of valuable information assets, resulting in copyright and intellectual property issues of concern to both vendors and users.

Compliance with IT-related legal and regulatory requirements and the effective use of legal contracts are clearly part of the effective control and oversight of IT activities by the Board of Directors and those charged with governance. All the regulations regarding IT strive for the same goals and these laws can be jotted down to their essential goals namely (ISACA, 2012:41):

- Establish and implement controls.
- Maintain, protect and assess compliance issues.
• Identify and remediate vulnerabilities and deviations.

• Provide reporting that can prove your organisation's compliance.

IT has to form an integral part of the company’s corporate governance due to its importance in the company. A corporate governance act is a detailed governance, risk and compliance system that synchronises governance with risk and compliance. It addresses all the issues within an entity relating to strategy, processes, technology and people (Petersen, 2013:3). Coetzee et al. (2010:2) asserted that corporate governance was implemented to eliminate fraud and to curb individuals whom were trading and making good money at the expense of the company’s stakeholders. The guidelines and acts of corporate governance were developed and issued by a number of influential companies throughout the world (Coetzee et al., 2010:8).

There are a lot of different governance regulations and most have incorporated IT governance. Each country has governing regulations for its companies to comply with.

In South Africa’s King report, guidelines of corporate governance were issued in response to the increasing concern about corporate failures and the perceived need for a formal code of corporate governance (Walker & Meiring, 2010:1). The King I report on corporate governance was published in 1994 by the Institute of Directors and the report aimed to assist companies and its directors by providing a comprehensive set of principles and guidelines to codify, clarify and elaborate on the common law principles of corporate governance. The King II report was issued in March 2002 and both reviewed and expanded on King I and had the same intentions as King I; to assist the companies and directors with corporate governance (Walker & Meiring, 2010:1). The King II report was then replaced by the third King code and this was due to the introduction of some new practices, including the composition and role of the Board of Directors, the Board committees and the emphasis of IT governance and the need to publish an integrated report (Muwandi, 2010:3).
Souabni (2011:1) states that companies only disclose the minimum information required by law or regulation; therefore companies may not be considering any risks that are not required by the law, acts or regulations. This may result in companies not acting upon or managing these risks that were left undisclosed. A study conducted by PwC (2014) supports this argument, where it was concluded that 80% of investors feel that the quality of the reporting of an organisation reflects the quality of its management. Perceptions of stakeholders contribute to and may affect companies’ reputations (IODSA, 2009:23).

This study makes the assumption that if companies are not mentioning anything about IT governance it will be due to misinterpretation or failure to understand the King III IT governance and disclosure requirements.

In addition to the corporate governance acts that were introduced, some countries introduced specific legislation to address corporate governance issues. The USA introduced SOX after the Enron and Worldcom scandals to prevent such scandals in the future and to protect the stakeholder’s investments. SOX was later adopted by the other G8 countries such as France, Germany, Italy and the UK (Coetzee et al., 2010:10). SOX is discussed in the course of this study even though South African companies are not legally compelled to comply to it. It is important in terms of corporate governance as some South African organisations, including public companies, have formal alliances with the USA through shareholding or business contracts thus the international audit firms operate across borders (Coetzee et al., 2010:10). Therefore SOX is an important corporate governance regulation to consider for many companies in South Africa. In order to assist in improving King III, such regulations that have an impact on South African companies are important to review. Improved and similar requirements of King III and SOX would also assist international companies that have to comply with both King III and SOX, making the preparation of annual reports easier without having to compare whether the entity complies with both regulations.

The other legislation discussed in this study includes the ISA 315 and the ISO’s legislation. The ISA 315 were established to provide guidance to the
auditors to obtain an understanding of the entity and its environment, including the internal controls of the organisation. The ISA 315 were first adopted by the European Union that includes some of the G8 countries (France, Germany, Italy and the UK). It was later adopted by the United Nations that include all the G8 countries and South Africa. ISA 315 are important to review in contribution to improving King III because it affects many South African companies since auditors have to comply with it (SAICA, 2015:315), while the ISO is the world’s largest international standard developer.

The norms established by ISO have a major impact on national and local environmental and social issues. It is essential to consider the ISO’s legislation even though it is used by companies on a voluntary basis, as most companies from different countries across the globe use the ISO’s legislation (Morikawa & Morrison, 2004:2). It may also contribute a great deal to the improvement of the King III report.

2.5.1 King III requirements for IT governance and disclosure

King III governs South African companies on corporate governance and disclosure and it was introduced due to the change of the Companies Act 2008 and also the change in the international governance trends, it became effective on the 1st of March 2010 (IODSA, 2009:2). The aim of King III was to place South Africa at the forefront of the governance internationally (Du Plessis, 2009:1). King III is the first King report to emphasise the importance of IT governance. The report is divided into different aspects and focuses on these by breaking each aspect down into different principles that must be applied and by applying these principles there are practices and recommendations to be followed (Du Plessis, 2009:1).

IT governance is among the aspects that the King III report focuses on. King III identifies that IT has turned out to be a fundamental part of doing business today, as it is important to the support, sustainability, and growth of organisations. IT cuts across all parts, components and processes in business and is therefore not only an operational enabler for a company, but a vital strategic asset which can be leveraged to generate opportunities and to gain
competitive advantage (Hoekstra et al., 2012:1). Therefore, King III deemed it fit to include the governance of IT in the report.

IT is part of a business strategy and the pervasiveness of IT in organisations mandating the governance and disclosure of IT is regarded as important as any governance and disclosure of other business risks found in the company’s annual reports (Hoekstra et al., 2012:1). As discussed above, it is clear that the complexity of IT creates operational risks, therefore in exercising their duty of care, directors should ensure that prudent and reasonable steps are taken with regard to IT governance, which should be disclosed to stakeholders. The requirements of IT governance as per the King III report are as follows (IODSA, 2009:22 and Nkonki, 2011:1 and PwC, 2015:1):

- The Board of Directors should be responsible for IT governance: The IT governance framework supports effective and efficient management and decision-making around the use of IT resources to facilitate the achievement of the company’s objectives and the management of IT-related risks

- IT should be aligned with the performance and sustainability objectives of the company: IT should be exploited in a way that most effectively supports and enables the business strategy, adds value and improves performance. The Board of Directors should ensure that the IT strategy is integrated into the company’s strategic and business processes and that IT adds value.

- The Board of Directors should delegate to management the responsibility of implementing an IT governance framework: Responsibility for the implementation of IT governance should be assigned to the Chief Information Officer (CIO), as appointed by the CEO. The CIO should act as an intermediary between the board and management on IT-related issues and should be the connection between IT and business. The CIO should report to the Board of Directors on the performance of the IT function.
• The Board of Directors should monitor and evaluate significant IT investments and expenditure: Value delivery and return on investment of IT should be monitored by the board.

• IT should form an integral part of the company’s risk management: The Board of Directors should evaluate how IT can be used to aid the company in managing its risk and compliance requirements.

• The Board of Directors should ensure that information assets are managed effectively: The Board of Directors should ensure that processes have been established to ensure a formal information security management system is in place.

• A risk committee and audit committee should assist the Board of Directors in carrying out its IT responsibilities: IT, as it relates to financial reporting and the status of the company as a going concern, should be the responsibility of the audit committee.

King III (IODSA, 2009:5) states that when companies are preparing their integrated annual reports, they should convey necessary and adequate information about the operations of the company. In the company’s integrated annual report, IT reporting should be included by the Board of Directors and should be complete, timely, relevant, accurate, and accessible and should contain prospective information (Nkonki, 2011:2). It can be concluded that all South African companies should comply with King III and disclose the governance of IT followed by their entity as it is good corporate governance.

Since IT is ever-changing and it is growing rapidly, it is essential to compare King III IT governance disclosure requirements with the international regulations to keep on par with international standards of corporate reporting.

2.5.2 SOX requirements for IT governance and disclosure

SOX is legislation that was passed on by the United States Congress to protect shareholders and the general public from accounting errors and fraudulent practices in the organisation, as well as to improve the accuracy of corporate disclosures. It came into force in 2002, created to rebuild public
trust in the corporate sector after the accounting scandals of Enron, Author Anderson and others in 2001 (McClimon, 2015:1).

The regulation requires all organisations in four of the great eight countries (France, Germany, Italy and the USA), large and small to adhere to the significant governance standards of SOX that increased Board members’ role in overseeing financial transactions and auditing procedures (Anon, 2003:1). Anon (2003:1) further pronounce that SOX requires a number of disclosures, including information on IT governance and internal control mechanisms.

In order to examine how SOX deals with the governance and disclosure of IT, two sections have to be considered, Section 302 and Section 404. Even though SOX consists of multiple sections and companies are required to comply with all, only these two section principles relate to IT.

Section 302 is a section intended to safeguard the company against faulty financial reporting and as part of this section, companies must safeguard their data responsibly as to ensure that financial reports are not established upon faulty data, interfered data, or data that may be highly inaccurate. Section 404 involves the safeguards mentioned in Section 302 to be available to the public and be reviewed by the external auditing (Correlog, 2011:2). The sections are further explained:

**Section 302:** This section requires the signing officers (the individuals or management with authorised signatory) to have disclosed to the auditor of the financial statements and the audit committee of the Board of Directors (or persons fulfilling the equivalent function) all major deficiencies in the policy or operation of internal controls. This could unfavourably affect the issuer's ability to record, process, summarise, and report financial data and indicated to the issuer's auditors any material weaknesses in internal controls.

The signing officers should indicate in the report whether or not there were noteworthy changes in internal controls or other factors that could significantly affect internal controls following to the date of its evaluation, including any corrective measures with regard to significant deficiencies and material weaknesses. Even though Section 302 does not specify which internal
controls are to be disclosed, it can be deduced that a company’s computerised internal controls form part of IT governance and need to be disclosed because most organisations are using IT-based systems for the day-to-day activities of the company.

**Section 404:** It requires that the annual reports should include an internal control report. The report shall state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting.

It should contain an assessment, from the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting. Although the topic of IT governance is not discussed specifically within SOX, effective and reliable internal control (referring to the procedures within the entity to ensure that the company achieves the targets set in the strategy) forms the basis for compliance and prudent business practices (Correlog, 2011:16). No internal controls would be complete without addressing IT governance. Companies regulated by SOX should therefore consider the IT governance when reporting the company’s performance (SOX, 2002:118 and Stults, 2004:4).

### 2.5.3 ISA 315 requirements for IT governance and disclosure

ISA 315 deals with the auditor’s responsibility to identify and assess the risks of material misstatement in the financial statements through understanding the entity’s environment and internal control (IFAC, 2010:264). It is a standard that is used in South Africa in terms of auditing and the international standard that all of the G8 countries comply with since it was adopted by the European Union and the United Nations. ISA 315 notes that many IS make use of IT and it consists of an infrastructure (physical and hardware components), software, people, procedures and the data. In accordance to ISA 315 paragraph 9, IS control activities are application controls that apply to the processing of single applications and general IT controls (SAICA, 2015:316). It is procedures and policies that relate to many applications and support effective functioning of application controls by helping to ensure the continued proper operation of IS.
ISA 315 then require the auditor to assess whether there are inconsistencies between the entity's IT strategy and its business strategies, changes in the IT environment and whether there are installation of significant new IT systems related to financial reporting (SAICA, 2015:315). The auditor is required to perform an assessment to obtain an understanding of the entity and its environment, including its internal controls because IT forms part of the entity's internal control.

South African Institute of Chartered Accountants (SAICA) understands the importance of good internal control therefore, if SAICA requires the auditor to take IT into consideration, it is an important internal control and it is recommended to be done by all companies. Hence, if companies apply and implement internal controls it is a sign of good corporate governance.

2.5.4 ISO requirements for IT governance and disclosure

ISO is an independent, non-governmental membership organisation and the world's largest developer of voluntary international standards (Anon, 2015:1). ISO sets voluntary standards that distil international expertise and good practice and was contributed by the people that understand the national and local environmental, social and the economic problems of the organisation (such as the directors of companies) and are best positioned to observe the standards in action and to maintain them (Anon, 2015:1). The ISO deals with IT governance and helps organisations keep information assets secure. Calder (2013:3) states that the role of IT in corporate governance, has become more important, and IT governance is increasingly recognised as a specific area for the Board of Directors and corporate attention. ISO 27000 requires companies to govern and disclose IT as follows (Calder, 2013:3):

- IT policies and objectives of the company in consideration of the strategic direction of the organisation.
- Establish a framework that clearly sets the objectives of the company and demonstrates the commitment of the company to meeting them.
• IT risk assessment analysis processes the realistic likelihood and potential consequences of IT-related risks and has levels that rank the risks determined.

• Information about technical vulnerabilities should be obtained and ensure appropriate measures are taken to address the risks.

• The policies and agreements to maintain the security of IT is transferred within and outside the organisation.

Even though the ISO is not enforceable but voluntary, the IT governance disclosure is clearly addressed and companies can govern and disclose IT in a manner that is also clear and understandable.

Even though all the regulations have the same intentions of protecting the confidentiality, integrity and availability of information that influence an organisation's stakeholders, each regulation is formulated differently and can therefore be interpreted differently depending on the country and the company. In order to understand the different regulations and to determine whether there are any similarities or differences in the manner in which the legislations can be interpreted, the comparison between King III, ISA 315, SOX and ISO are conducted in Table 2.1.

2.6 COMPARISON OF THE KING III WITH THE INTERNATIONAL REGULATIONS WITH REGARD TO IT GOVERNANCE AND DISCLOSURE

In order to determine whether the King III should be improved that it may be clearly understood and interpreted by the users of the code and to have a competitive advantage and effectiveness of corporate governance, it has to be compared to other regulations. Proper IT governance has become the absolute expectation of management by the company stakeholders. Table 2.1 is the compilation of the requirements according to the different regulations discussed above.
### Table 2.1: Comparison of the regulations

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The Board Of Directors is responsible for IT governance (IODSA, 2009:19).</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>IT has been aligned with the performance and sustainability objectives of the company (IODSA, 2009:19).</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>The Board Of Directors should delegate to management the responsibility of the implementation of an IT governance framework (IODSA, 2009:19).</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>The Board of Directors monitors and evaluates significant IT investments and expenditure (IODSA, 2009:19).</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>IT is an integral part of the company’s risk management plan (IODSA, 2009:19).</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>The Board of Directors ensures that information assets are managed effectively (IODSA, 2009:19).</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>--------------------------</td>
<td>----------------------------------------</td>
<td>--------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>A risk committee and audit committee assists the Board of Directors in carrying out its IT responsibilities (IODSA, 2009:19).</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>X</td>
</tr>
<tr>
<td>Establish safeguards to prevent data tampering (Correlog, 2011:2).</td>
<td>X</td>
<td>√</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Establish safeguards to ensure the effectiveness of the IT controls (Correlog, 2011:2).</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Establish verifiable controls to track data access (Correlog, 2011:2).</td>
<td>X</td>
<td>√</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Access inconsistencies between the entity’s IT strategy and its business strategies (SAICA, 2015:315).</td>
<td>√</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Report any changes in the IT environment and if there are installations of significant new IT systems related to financial reporting (SAICA, 2015:319).</td>
<td>√</td>
<td>X</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Establish IT risk assessment analysis processes that assesses the realistic likelihood and potential consequences of IT-related risks and have levels that rank the risks determined (BSI 2013:3).</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>√</td>
</tr>
<tr>
<td>Information about technical vulnerabilities should be obtained and ensure appropriate measures are taken to address the risks (BSI 2013:3).</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>The policies and agreements to maintain the security of IT are transferred within and outside the organisation (BSI 2013:3).</td>
<td>X</td>
<td>√</td>
<td>X</td>
<td>√</td>
</tr>
</tbody>
</table>

The table indicates the differences and similarities in King III and the other defined regulations. The first requirement is that the Board of Directors is responsible for IT governance which is a requirement according to King III. ISA 315 agrees with King III while the other regulations only state that the company has to have IT governance but does not set out who is responsible for it.

All four regulations agree that IT has to be aligned with the performance and sustainability objectives of the company. Although ISO does not mention the party responsible for IT governance in the company, it agrees with King III and ISA 315 that the Board of Directors may delegate to management the responsibility for the implementation of IT, while SOX does not indicate anything about the delegation or responsibility of IT governance.
King III clearly indicates that the Board of Directors is responsible for monitoring and evaluation of the significant IT investments and expenditures, while the other three regulations do not specifically indicate who is responsible for monitoring and evaluating the company’s IT investments but it does state that the IT investments and expenditures should be governed and disclosed. All four regulations state that IT is an integral part of the company’s risk management plan. King III again delegates to the Board of Directors the management of information assets and the other three regulations do not discuss anything about the management of information assets.

King III, SOX and ISA 315, state with regard to management of IT-related risks, that the risk committee and the audit committee may assist the Board of Directors while the ISO does not discuss anything about IT risk management. SOX’s requirements specifically states that the companies should establish safeguards that prevent data tampering. No other regulation specifies the need of safeguards that prevent data tampering. All four regulations require establishment of safeguards that ensure effectiveness of the IT controls. The SOX also requires that companies establish verifiable controls to track data access.

The three regulations excluding the SOX require that companies provide access to and disclose any inconsistencies between the entity’s IT strategy and its business strategy and also the changes in the IT environment and if there are any new installations of significant IT systems related to financial reporting. According to ISO the company should establish an IT-related risk assessment analysis process which assesses the realistic likelihood and potential consequences of IT-related risks and have levels that rank the determined risks. The other three regulations require the companies to assess the risks but do not specify whether these risks should be measured and ranked. Another requirement that all four regulations agree on is that the information about the technical vulnerabilities should be obtained and appropriate measures should be taken to address the risks. ISO and the SOX state that the policies and agreements to ensure the security of IT should be transferred within and outside the organisation.
In order to be more comprehensible and assist companies, King III should therefore address the differences from the other regulations and these differences are as follows:

- State that companies should establish safeguards to prevent data tampering.
- State that companies should establish verifiable controls to track data access.
- State that all companies should have an IT risk assessment analysis process which assesses the realistic likelihood and potential consequences of IT-related risks and has levels that rank the determined risks.
- State that companies should disclose policies and agreements to maintain the security of IT and these policies should be transferred within and outside the organisation.

King III has to clearly indicate some of the risks and procedures that should be disclosed with regard to IT as indicated in the previous discussion. The King III report clearly indicates that the Board of Directors is responsible for IT governance but does not explicitly state information regarding technical vulnerabilities that should be obtained and communicated within and outside the entity (disclosed in the company’s annual reports). The differences pointed out above are as per the different regulations used or applied in different countries. King III did not address the requirements and did not discuss other requirements that could make the report clear and understandable; therefore to clarify the requirements of King III the above-mentioned differences should be implemented.

2.7 COMPREHENSIVE SUMMARY AND CONCLUSION

This chapter dealt with the literature review, where the history of IT and its evolution over the past years since 1950, is discussed. The influence that IT has on the entities is also discussed, as well as the risks that were introduced by the ever-changing IT environment.
After the risks were identified it was necessary and of utmost importance to introduce the governance of those risks. This chapter also addresses the history and backgrounds of the regulations that were implemented by different countries to try and assist organisations to understand the methods and requirements of effective IT governance.

The literature study also identified the IT governance framework that was established for all entities to follow, namely COBIT. All countries have to draft their regulations with this framework as the base. Previous studies stated that it is clear that the King III report is in accordance with COBIT requirements. An analysis was also conducted to determine the differences between the four regulations, namely King III, ISO, SOX and ISA 315. It was evident that King III has some similarities with other regulations and some differences. King III is also not too clear on what information about technical weaknesses, which should be obtained and communicated within and outside the entity, should be disclosed. Furthermore it is vague regarding what policies and agreements of IT should be disclosed in the company’s annual reports. Therefore a further study is conducted to evaluate to what extent the top 40 JSE listed companies comply with the King III report. This evaluation is to determine as to whether the entities understand the requirements of King III. Thereafter it is concluded whether there is a need for improvement of King III companies’ disclosure of IT governance.
CHAPTER 3
RESEARCH METHODOLOGY

3.1 INTRODUCTION

The literature review in Chapter 2 of this study discussed the importance of IT that indicates that all companies in today’s business environment make use of IT in their day-to-day running of business. Chapter 2 also emphasised that, due to the risks caused by the use of IT, governance of IT is essential. Therefore the four selected regulations (King III, ISO, SOX and ISA 315) that are used in different countries to govern IT were discussed. A comparison of these four different regulations governing IT governance and disclosure was also conducted to make a clear distinction between the regulations’ differences and similarities. This comparison was also conducted to gain a clear understanding on how King III can be improved so that all companies may have a better understanding of what to disclose in order to comply with the IT governance and disclosure requirements. This chapter defines research and explains the characteristics thereof. The research methodology applied in this study is also presented.

Somers (2012:2) and Maree and Van der Westhuizen (2013:31) define research as a systematic investigation of a study through a process of collecting materials, sources and data in order to analyse and interpret the information to establish facts, gain insight about the phenomenon which is of interest, and to reach new conclusions. Dane (2011:3) simplifies the definition of research to a procedure of questioning and attempting to answer the questions about the world. The process of asking and attempting to answer the questions involves different methods that include questionnaires, interviews, experiments, analysis or sometimes a combination of these methods (Dane, 2011:3).

According to Keohane (2014:2) and Leedy and Ormrod (2014:2) research has distinct characteristics and can be explained as follows:
• It originates from a question or a problem.
• The research goal is inference.
• It requires an articulated plan for proceeding.
• It usually divides the main problem into more manageable secondary objectives.
• Research is usually guided by a specific research main objective, question or a problem statement.
• The conclusions of research are uncertain critical assumptions.
• The content of research requires the collection, analyses and interpretation of data in an attempt to solve or reach a different conclusion of the problem that initiated the research.
• Research is, of its own nature, unique or more exactly convoluted.

In order to achieve the research objective of identifying the extent to which the top 40 JSE listed companies comply with the King III IT governance and disclosure requirements, certain research methodologies were utilised in this study. Hence this chapter provides a full description of the research methodology followed. The main aim of this chapter is to render an in depth explanation of research design, research methodology, validity and reliability, data collection methods, ethical considerations, and data analysis.

3.2 RESEARCH DESIGN

A research design is significant because it assists the researchers to strategise their overall research study in a purposeful manner in order to obtain relevant data for their research problem (Leedy & Ormrod, 2014:4) In agreement with Leedy and Ormrod (2014:4), Denzin and Lincoln (2000:22) describe research design as a flexible set of guiding principles that firstly link theoretical models to strategies of inquiry and secondly to methods for collecting empirical material.

According to the social scientists Perri and Bellamy (2012:20), research design can be described as:
The specification of the methods in which data were created, collected, coded, analysed and interpreted.

To enable the researcher to draw warranted descriptive, explanatory or interpretive inferences.

Where the warrant is calculated to set a reasonable trade-off between competing virtues.

Where the standards of warrant may vary slightly, but are based on a core set of virtues for each type of inference.

According to Leedy and Ormrod (2014:240) there are a variety of research designs that have emerged and that differ in the extent to which the researcher uses the different variables. These research designs are divided into five categories (Leedy & Ormrod, 2014:240), and these categories are as follows:

- **Pre-experimental designs:** these designs are only helpful when developing uncertain hypotheses that should be followed up with more controlled studies.

- **True experimental designs:** these designs offer a greater level of control and as a result there is greater internal validity.

- **Quasi-experimental designs:** these designs take whatever variables the researcher had not controlled into consideration when interpreting the data.

- **Ex post facto designs:** these designs present events that have already occurred or conditions that are already in existence.

- **Factorial designs:** these designs examine the effects of two or more independent variables in a single study.

The research design used in this study is the ex post facto design because compliance with the King III report’s IT governance requirements already exist. The main goal of this study is to learn about companies’ understanding of the King III IT governance and disclosure. Inferences about the companies’
understandings are drawn from the individual company’s annual reports published for the public view.

3.2.1 Research Paradigms

Barker (2003:312) regards paradigm as a model or pattern containing a set of legitimated assumptions and a design for collecting and interpreting data. In agreement with Barker’s definition, Creswell (2007:19) defines a paradigm as a basic set of beliefs that guide action or a frame of reference used to organise observation and reasoning. Denzin and Lincoln (2000:19) set paradigm out as a term of the net that contains the researcher’s epistemological, ontological and methodological premises.

Research is interpretive therefore it is directed by a set of beliefs and feelings that deal with two extremes which are interpretivist and positivist (Denzin & Lincoln, 2000:19). The interpretivism paradigm provides insight to the behaviour displayed, meanings and interpretations (De Vos et al., 2011:311). Maree and Van der Westhuizen (2009:20) describe the interpretivism paradigm as the adoption of views by the researcher and there are no fixed truths to these views.

The positivist approach is opposed by the anti-positivists (interpretisists) who share a resistance to uphold the natural-scientific method as the norm in human behavioural research (Welman et al., 2007:6). Positivism as reported by Denscombe (2008:14) can be defined as an approach to social research that aims to apply the natural science technique of research to investigations of social phenomena and explanations of the social world. Paradigms that are used by qualitative researchers vary, depending on the set of beliefs they bring to research. The full description of the methodology used in this study follows in Paragraph 3.3. The different methodologies are explained and the reasons for choosing the specific methodology are discussed.

3.3 RESEARCH METHODOLOGY

Methodology is the approach of using appropriate techniques in a correct format or way. It also entails how well the arguments are articulated and
analysed from raw data collected along with how well the conclusion is drawn (Perri & Bellamy, 2012:11). The data gathered are very important for the researcher as the data play a critical role in the study in terms of what research methodology should be followed (Leedy & Ormrod, 2014:95). Leedy and Ormorod (2014:96) simplifies the definition of research methodology to the extraction of meaning from raw data.

Methodology is about arguments that show a warrant for inferences, because to be able to draw sound conclusions all depends on designing all stages of the research study on sound methodological principles (Perri & Bellamy, 2012:12). There are two types of methodologies, the quantitative and the qualitative. The quantitative approach is also known as the positivist approach while the qualitative approach is also known as the anti-positivist approach (interpretivist).

Berg and Lune (2014:3) state that qualitative research refers to meanings, concepts, definitions, characteristics, metaphors, symbols, and descriptions of things. On the other hand quantitative research refers to the calculation and measure of things and the extents and distributions of the subject matter. De Vos et al. (2011:66) identify that even though there is a distinction between quantitative and qualitative researchers, it does not mean that these methods are mutually exclusive as some researchers prefer to use both approaches that is called a mixed methods research approach.

The collection of qualitative data is a natural setting, sensitive to the people and places under which the study occurs and data analysis is inductive and establishes patterns (Creswell, 2007:19). This suggests that qualitative data can be systematically collected, organised, interpreted, analysed and communicated in order to address real world problems (Tracy, 2013:5). Tracy (2013:6) further states that the qualitative research approach can provide knowledge that targets societal issues, questions, or problems and therefore serves humankind.

Welman et al. (2007:135) indicate that the quantitative measurement and data collection procedures are based on systematic observation. Systematic
observation means that the work is replicable, meaning that independent observers other than the researcher should also be able to observe and report what the researcher has observed and reported (Welman et al., 2007:135). Maree and Pietersen (2014:263) indicate that the quantitative research approach relies on numerical data to test the relationship between the variables.

Table 3.1 provides a comparison (De Vos et al., 2011:66 and Saunders et al., 2000:381) between the quantitative and the qualitative approach.

**Table 3.1: A comparison between the qualitative and the quantitative approach**

<table>
<thead>
<tr>
<th>Quantitative approach</th>
<th>Qualitative approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Epistemological roots in positivism meaning the data are derived from numbers.</td>
<td>Epistemological roots in phenomenology, more broadly it is referred to as interpretivism, which means that the data is conveyed through words.</td>
</tr>
<tr>
<td>The purpose is to test analytical and cause and effect hypotheses about social reality.</td>
<td>The purpose is to create a comprehensive description of social reality.</td>
</tr>
<tr>
<td>Data collection methods utilise deductive logic, which indicates that the conceptual and theoretical structure is developed and then tested by empirical observation.</td>
<td>Data collection methods utilise inductive logic, meaning that the theory is developed from the observation of empirical reality.</td>
</tr>
<tr>
<td>Concepts are changed into operational definitions and result analysis is conducted by means of statistical language (diagrams and statistics).</td>
<td>Participants’ natural language is applied in order to come to a understanding of their words. Analysis is expressed by means of conceptualism.</td>
</tr>
</tbody>
</table>
Table 3.1: Quantitative and Qualitative Approaches

<table>
<thead>
<tr>
<th>Quantitative approach</th>
<th>Qualitative approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>The research design is standardised</td>
<td>The research design is flexible and</td>
</tr>
<tr>
<td>according to a fixed process and can be</td>
<td>distinctive throughout the research</td>
</tr>
<tr>
<td>duplicated.</td>
<td>process. There are no fixed steps that</td>
</tr>
<tr>
<td></td>
<td>could be followed and the design</td>
</tr>
<tr>
<td></td>
<td>cannot be duplicated.</td>
</tr>
</tbody>
</table>

Source: De Vos et al. (2011:66) and Saunders et al. (2000:381)

The above-mentioned characteristics influenced the research methodology, research design and data collection methods of this study and the study therefore followed a mixed method research approach.

The qualitative research approach was followed in order to understand the disclosure requirements of IT according to the different regulations used in different countries. The qualitative approach also helped to grasp the differences between how the ISO, ISA 315, SOX and the King III report require companies to disclose IT governance. The differences indicated are used as recommendations in Section 5.4 that can be implemented by the King III report for it to be specific and clear to the users.

The quantitative research approach in this study was followed in order to evaluate the top 40 JSE listed companies, to calculate the percentages of companies that comply and those that do not comply with the individual IT governance disclosure requirements. The evaluation was also done in order to obtain an overall percentage of companies that fully comply, partially comply and those that are non-compliant to the King III IT governance and disclosure requirements. This further assisted to determine whether companies clearly understand the requirements of IT governance and disclosure in terms of the King III report. The analysis of the top 40 JSE listed companies will be performed in Section 4.4.

3.4 VALIDITY AND RELIABILITY

Validity is when an instrument measures that which it is supposed to measure, while reliability has to do with the consistency or repeatability of a measure or
instrument (Maree & Pietersen, 2014:147). In accordance to Van Zyl (2014:123) validity refers to the outcomes of the test and not the test itself. Van Zyl (2014:127) further states that the relationship between reliability and validity is direct and easy to understand because reliability is necessary yet not sufficient on its own but it is conditioned to validity. In other words, a test can be reliable but not valid, but a test cannot be valid without being reliable. Saunders et al. (2000:101) explained validity as being concerned with whether the findings are really about what they appear to be about.

Therefore the definition of validity expressed by the different authors has a similar meaning and the same goes for the definition of reliability. In accordance to Saunders et al. (2000:100) reliability can be evaluated by asking two questions that relate to the two methods that the researcher can use. The quantitative and qualitative methods have different questions when it comes to evaluating reliability and the questions are as follows:

- Will the measure yield the same results if done differently or under different circumstances? (This is quantitative because it is a systematic observation meaning that the work can be duplicated. It is only based on figures and can be done by different individuals and still obtain a report with the same interpretation of the results).

- Will similar observations be made by different researchers on different occasion? (This is qualitative because it is flexible, distinctive and cannot be duplicated. The exact observation cannot be produced but the results may be similar).

Validity and reliability works differently depending on the methodology followed by the study because, according to Maree and Pietersen (2014:80), reliability and validity are crucial aspects in quantitative research, while in qualitative research the researcher is the data-collating instrument. Since this study includes both a qualitative and a quantitative methodology, the validity and reliability of the study can only be determined once the analyses of the top 40 JSE listed results are processed. The analysis was conducted to evaluate the companies’ understanding of the IT disclosure and governance requirements of King III.
3.5 DATA COLLECTION METHODS

In accordance to Van Zyl (2014:156) the data collection process involves everything from obtaining possible resources and arranging the collection of data to the actual recording of the data in some type of form that assists the researcher to organise this information and facilitate the data analysis process. Maree and Pietersen (2014:78) states that data collection is done in different ways. This study collected data by means of a qualitative and quantitative approach by means of studying documents and performing secondary analysis. The King III report’s IT requirements were studied and used as the basis for evaluating the top 40 JSE listed companies.

3.5.1 Population

Saunders et al. (2000:150) defines population as the full set of cases from which the sample is drawn from. In agreement with Saunders et al. (2000:150) definition of population Van Zyl (2014:33) also defines population as the larger group where the sample is drawn from, in other terms population is the entire group of potential participants to whom the researcher wants to generalise the results of the study.

One of the purposes for this study is to determine whether the King III report needs improvement for all the users to understand and fully comply with the report in terms of the IT governance and disclosure requirements. This was done by evaluating the top 40 JSE listed companies. A literature study was first conducted to assist in the comparisons between the different IT regulations that are used in different countries and a conclusion was made that all the regulations deal with IT governance and disclosure but have different requirements, reads differently and can be interpreted differently. The companies in question constitute 40 entities. The number of these companies was taken from the JSE listing of the main board.

3.5.2 Sample

Van Zyl (2014:33) defines a sample as the smaller group selected from the population. The sample should be drawn from the population in such a
manner that it would maximise the likelihood that the sample will represent the population as much as possible (Van Zyl, 2014:33). Concurring with Van Zyl (2014:33) De vos et al. (2011:223) refer to a sample as elements or a subset of the population considered for actual inclusion in the study, or it can be regarded as a subset of measurements drawn from a population in which the researcher is interested in. When the sample does represent the population, the results of the study are said to be generalisable or to have generalisability (Van Zyl, 2014:33).

In this study a non-probability sample was drawn from the top 40 JSE listed companies from the market capitalisation of the All Share Index on the JSE, and the sample represents the complete population of the top 40 JSE listed companies. Out of the top 40 JSE listed companies all of the companies were selected (100 per cent) and used in this study.

The top 40 JSE listed companies were used as the basis of the study as these companies have to comply with King III requirements (JSE, 2012:6). These companies are the biggest companies in South Africa and truly represent the diverse industries of the country. As these are the top companies, smaller and rising companies desire the governance and disclosure of these top companies. The companies selected for this study were the top 40 publicly listed companies on the JSE on the 31st March 2015 and the annual reports were publicly available online. The latest publicly available annual reports of the selected companies because the King III became effective in 2010 therefore the annual reports published years before 2010 could not be compliant of the King III and the companies have different reporting periods, causing some companies’ 2014 and 2015 annual reports to be used, due to companies having six months after year-end to finalise their annual reports (National Treasury, 2012:10).

The decision to use reports of the period of 31st March 2015 was based on the latest publicised top 40 JSE listed companies when the study began. It was also essential to use the latest publicly available annual reports of the companies because companies have different year-ends and not all of the 2015 statements are readily available. According to the literature review
conducted in the previous chapter, IT is currently used by all companies, therefore the governance and disclosure thereof is important. All of the top 40 JSE listed companies were used; no sector or industry was omitted.

3.6 ETHICAL CONSIDERATIONS

Saunders *et al.* (2000:130) argues that ethical consideration refers to the appropriateness of the researchers’ behaviour in relation to the rights of the participants used during the study. The researchers’ behaviour should ensure that the rights of the participants are not affected by the study and should ensure throughout the study that participants remain unaffected. Creswell (2015:168) also mentions that even data collection should be ethical and respect individuals, sites and companies. Obtaining permission before the collection of data is not only a part of the informed consent process but also an ethical practice (Creswell, 2015:168).

It is important that the author protects the rights of the participating companies and ensures that there is no violation of their rights. All ethical concerns were considered by the author, and the author is confident that no ethical issues will arise in the study because the annual reports that are publicly available were used and there will be no alterations to the annual reports. The author used numerical values (e.g. Company 1 for the first of the top 40 JSE listed companies) in order to keep the companies’ confidential and unviolated.

3.7 DATA ANALYSIS

Maree and Pietersen (2014:183) reason that after the information has been collected and captured on computers as numbers called raw data, the analysis process then follows with descriptive statistics or summarising the raw data as meaningful and understandable information. The annual reports of the companies were analysed by comparing the disclosure of IT governance in the individual company’s annual reports to the requirements of the King III report.

King III report has seven IT governance requirements that companies need to comply with. Self-developed compliance requirement questions were used in
this study and the compliance requirements are based on the standard IT governance requirements set out by King III. The compliance test requirements are as follows:

- Is it disclosed in the company’s annual report that the Board of Directors are responsible for the IT governance of the company?

- Is it disclosed in the company’s annual report that the IT governance is aligned with the performance and sustainability objectives of the company?

- Is it disclosed in the company’s annual report that the Board of Directors delegate the responsibility to implement an IT governance framework to management?

- Is it disclosed in the company’s annual report that the Board of Directors monitor and evaluate the significant IT investments and expenditure?

- Is it disclosed in the company’s annual report that IT forms an integral part of the company’s risk management?

- Is it disclosed in the company’s annual report that the Board of Directors ensure that information assets are managed effectively?

- Is it disclosed in the company’s annual report that the risk committee and the audit committee assist the Board of Directors in carrying out its IT responsibilities?

These seven compliance test requirements are compared against the top 40 JSE listed companies’ annual reports to determine whether they mention or comply with any of the seven IT governance requirements.

The purpose of the compliance test requirements was to evaluate the extent to which the top 40 JSE listed companies comply with King III’s IT governance and disclosure requirements. Non-compliance with the regulations refers to intentional or unintentional act, in which unintentional refers to misunderstanding or misinterpretation of the laws and regulation (Marx et al., 2011:279). For the purpose of this study the assumption was made that companies that do not comply with the IT governance and disclosure
requirements do not comply because these companies do not understand or misinterpret the King III report’s IT governance and disclosure requirements.

This evaluation provides a clear understanding of whether the companies understand and correctly interpret the King III report. The results obtained from this analysis were used to conclude as to whether the King III report needs to be improved or not.

3.8 COMPREHENSIVE SUMMARY AND CONCLUSION

The main aim of Chapter 3 was to clearly outline the research design and methodology followed in this study. The preceding discussions clearly indicated the importance of research design because it helps the researcher to manage overall study in a focused manner so that relevant data to a research problem can be obtained. This chapter also dealt with the definition of research methodology and it was defined as the technique used by the researcher to extract data from raw material. This study therefore follows a mixed methodology.

This chapter also clarified the procedures followed during the study and the reason for using the selected procedures. It also discussed the data collection methods used. Data collection is the process that involves everything from obtaining possible resources and process the data to a meaningful study. The population, which is also the sample in this study, was discussed in depth. A hundred per cent sample of the population was used because the population size was small and manageable. The sample is based on a non-probability sampling of the top 40 JSE listed companies. It was also concluded that the validity and reliability of the study could not be determined in this chapter but can only be determined once the analyses of the top 40 JSE listed results are processed.

Ethics needs to be considered when conducting a study, to ensure that the participants of the study are not affected and the rights of the participants are not violated. Therefore it was concluded that the participants of this study will not be affected because the annual financial statements are publicly available, no information was altered and the company names are left anonymous. The
last part that was discussed in this chapter was the data analysis procedures used in this study which is the analysis of the top 40 JSE listed companies.

The evaluation of the top 40 JSE listed companies is needed, because Chapter 2 found that King III is vague as to how the companies should govern and disclose IT governance and which information about technical weaknesses should be obtained and reported within and outside the organisation. Therefore an analysis in Chapter 4 discusses to what extent companies should comply with the IT governance and disclosure requirements of the King III.

Apart from the differences drawn from the comparison of the different regulations that was conducted in Chapter 2 and the conclusion that reflected that King III needs to improve, the analysis that is conducted in Chapter 4 also helps to establish whether it is necessary to improve the King III through the companies’ compliance with the disclosure requirements.
CHAPTER 4
DATA ANALYSIS AND FINDINGS

4.1 INTRODUCTION

The background to the study in Chapter 1 and the literature review conducted in Chapter 2 state that IT forms an integral part of the effectiveness and efficiency of a business. In the preceding chapters, the importance of IT governance and disclosure were discussed, therefore it is important to evaluate whether the companies comply with the requirements of IT governance and disclosure in accordance with the King III report. This chapter provides the data analysis and findings as to whether the top 40 JSE listed companies comprehend or misinterpret the King III report’s IT governance and disclosure requirements and if there is a need to improve the King III report. This data were obtained through the analysis of the top 40 JSE listed companies’ latest annual report. The data facilitates scrutiny of the top 40 JSE listed companies to see if they disclose their governance.

4.2 RECOMMENDED IT GOVERNANCE AND DISCLOSURE REQUIREMENTS

Salido and Voon (2010:3) asserts that IT governance describes how data are controlled within an organisation in order to meet regulatory, environmental and operational requirements. The regulatory requirements to be met in South Africa are in accordance with the King III report. In today’s corporate governance, IT is in the spotlight with regard to compliance, because many companies do not comply with the IT governance and disclosure requirements (ISACA, 2011:14).

PwC (2015:2) reasons that for a company to be able to gain stakeholder value, it should set out IT governance regulations that manage the IT department of the company effectively and efficiently.
The King III report is the recommended IT governance and disclosure requirements that South African companies should abide with. A conclusion can be drawn from the compliance disclosure of companies as to whether the companies comprehend or misinterpret the requirements and whether there is a need for King III to improve and clarify its requirements with regard to IT governance and disclosure.

4.3 RECOMMENDED IT GOVERNANCE RISK DISCLOSURE REQUIREMENTS FOR THE PURPOSE OF TESTING

All entities, regardless of size or structure, require a way to ensure that the IT function of the company sustains the organisation’s policies and goals (Schwartz, 2007:1). Schwartz (2007:1) further enunciates that the level of sophistication applied to IT governance may vary according to size, industry or relevant regulations. In general, the larger and more regulated the organisation, the more detailed the IT governance structure should be.

The King III report indicates that companies have to comply with the governance requirements or declare why they do not apply (IODSA, 2009). Even though the JSE published some guidelines to which listed companies have to comply with, none of the King III IT governance principles are mandatory according to the JSE guidelines, but since the IT principles have an impact on overall company governance, it has to be disclosed (Giles, 2013:1). Giles (2013:1) further mentioned that even though listed companies do not have to disclose IT governance as per JSE requirements, they still have to comply with the King III. Thus the companies still need to abide by the regulations or declare as set forth by the King III report why they do not comply. In this study the assumption is made that if the companies are not disclosing the information, the companies are not complying with the King III IT requirements.

Table 4.1 (column one) sets out the IT governance requirements for companies to comply with as recommended by the King III report published in 2009. This is used as a test in order to evaluate compliance therewith.
The table’s second column indicates the compliance requirements formulated based on the test that was developed in Chapter 3 Section 3.7. The test was developed to evaluate whether the companies comply with IT governance and if IT requirements should be clearly stated in the company’s annual report. The test is of a “yes” or “no” nature where an attribute is either present or not. The last column in the table indicates the paragraph numbers where the findings and recommended requirements are further discussed.

**Table 4.1: Recommended IT governance risk disclosure requirements for the purpose of testing**

<table>
<thead>
<tr>
<th>TEST (IODSA, 2009)</th>
<th>COMPLIANCE REQUIREMENTS (Self-developed)</th>
<th>PARAGRAPH</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The Board of Directors should be responsible for IT governance.</td>
<td>Is it disclosed in the company’s annual report that the Board of Directors is responsible for the IT governance of the company?</td>
<td>4.4.1</td>
</tr>
<tr>
<td>2. IT should be aligned with the performance and sustainability objectives of the company.</td>
<td>Is it disclosed in the company’s annual report that the IT is aligned with the performance and sustainability objectives of the company?</td>
<td>4.4.2</td>
</tr>
<tr>
<td>3. The Board of Directors should delegate to management the responsibility to implement an IT governance framework.</td>
<td>Is it disclosed in the company’s annual report that the Board of Directors delegates to management the responsibility to implement an IT governance framework?</td>
<td>4.4.3</td>
</tr>
<tr>
<td>4. The Board of Directors should monitor and evaluate significant IT investments and expenditure.</td>
<td>Is it disclosed in the company’s annual report that the Board of Directors monitors and evaluates the significant IT investments and expenditure?</td>
<td>4.4.4</td>
</tr>
<tr>
<td>TEST (IODSA, 2009)</td>
<td>COMPLIANCE REQUIREMENTS (Self-developed)</td>
<td>PARAGRAPH</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>5. IT should form an integral part of the company’s risk management.</td>
<td>Is it disclosed in the company’s annual report that IT forms an integral part of the company’s risk management?</td>
<td>4.4.5</td>
</tr>
<tr>
<td>6. The Board of Directors should ensure that information assets are managed effectively.</td>
<td>Is it disclosed in the company’s annual report that the Board of Directors ensures that information assets are managed effectively?</td>
<td>4.4.6</td>
</tr>
<tr>
<td>7. A risk committee and audit committee should assist the Board of Directors in carrying out its IT responsibilities.</td>
<td>Is it disclosed in the company’s annual report that the risk committee and the audit committee assist the Board of directors in carrying out its IT responsibilities?</td>
<td>4.4.7</td>
</tr>
</tbody>
</table>

### 4.4 RESEARCH FINDINGS OF COMPLIANCE WITH IT GOVERNANCE AND DISCLOSURE

The detailed results of the companies tested are listed in Appendix A. The research results for each IT governance and disclosure requirement is detailed and explained in the following sections.

#### 4.4.1 The Board of Directors should be responsible for IT governance

In order for companies to comply with the IT governance and disclosure requirement that states that the Board of Directors should be responsible for IT governance, the entity should ensure that they have stated either of the following statements in their annual reports (PwC, 2015:1):

- That the IT governance framework is established in the entity.
• State that the IT governance is part of the company’s Board of Directors’ agenda.

The graph below sets out the percentages of the top 40 JSE listed companies that do comply and the companies that do not comply with this IT governance requirement in their annual reports.

**Graph 4.1: Results of the requirement stating that the Board of Directors should be responsible for IT governance**

![Graph showing compliance rates for IT governance requirement]

The results declare that a total number of 19 out of the 40 companies JSE listed companies (47%) did comply with the first requirement of IT governance disclosure, while 21 out of 40 companies (53%) failed to mention this requirement in their annual reports.

**4.4.2 IT should be aligned with the performance and sustainability objectives of the company**

In the background study in Chapter 1, the importance of IT was discussed, where it was stressed that IT in today's business environment is aligned with the performance and sustainability objectives of the entity. In order for companies to fully comply with the IT governance disclosure it has to be stated, in their annual report, how the IT within the company is aligned with the performance and sustainability objectives of the company. Some of the
examples for complying with this requirement (KPMG, 2009:6) are to state either of the following:

- State that the IT strategy is integrated with the company’s strategic and business processes.
- That the IT value proposition is defined, maintained and validated by the organisation.
- State that specific consideration is given to all the negative impacts that IT could have on the business environment of the company.
- State that there is a process in place to identify and to exploit opportunities to improve the performance and sustainability of the company through the use of IT.

Graph 4.2 represents the results obtained from the evaluation of the top 40 JSE listed companies for the compliance of the second requirement in the IT governance and disclosure requirements in accordance with the King III report recommendations.

Graph 4.2: Results of the requirement stating that IT should be aligned with the performance and sustainability objectives of the company
In Graph 4.2 the results indicate that 21 out of the 40 JSE listed companies (52%) comply with the second requirement of aligning the performance and sustainability objectives of the company with IT, while 19 of the 40 companies (48%) do not meet this requirement.

4.4.3 The Board of Directors should delegate to management the responsibility to implement an IT governance framework

The Board of Directors should acquire assistance within the organisation with IT governance and the implementation of the company’s IT framework. Graph 4.3 displays the results obtained in the analysis conducted. The company should therefore disclose either of the following in its annual report to comply with this requirement (Roos, 2012:7):

- State that the responsibility for implementation of the structures, processes and mechanisms for the IT governance framework is delegated to management.
- State that the Board of Directors have appointed an IT management committee or similar function to assist with its governance of IT.
- Disclose that the company’s CEO has appointed a CIO responsible for the management of IT.
According to Graph 4.3, only 17 of the 40 JSE listed companies (42%) evaluated comply with the disclosure of the requirement that the Board of Directors should delegate to management the responsibility to implement the IT governance framework of the company. On the other hand 23 of the 40 companies (58%) do not state this requirement in their annual reports and are therefore non-compliant to the third requirement of King III’s IT governance and disclosure requirements.

4.4.4 The Board of Directors should monitor and evaluate significant IT investments and expenditure

In order to fully disclose IT governance and be fully compliant, companies also need to comply with the requirement that the Board of Directors should monitor and evaluate the significant IT investments and expenditure of the entity. The recommendations for complying with this requirement (Roos, 2012:8) are as follows:

- In the annual reports the company should disclose the amount spent on, and the value gained from IT.
The annual reports should state that the Board of Directors oversees value delivery in IT and monitors the return on investments from significant IT projects.

It should be stated in the company’s annual report that the Board of Directors ensures that intellectual property contained in information systems are protected.

Also disclose in the company’s annual report that the Board of Directors obtained an independent assurance on the IT governance and controls supporting outsourced IT services.

Graph 4.4 illustrates the results attained from the evaluation conducted of IT governance compliance fourth requirement.

**Graph 4.4: Results of the requirement stating that the Board of Directors should monitor and evaluate significant IT investments and expenditure**

The results illustrated in Graph 4.4 indicate that 17 out of the 40 JSE listed companies (42%) comply with the fourth requirement. Whereas 23 out of 40 companies (58%) do not comply with the requirement that states that the
Board of Directors is responsible for monitoring and evaluating significant IT investments and expenditure of the entity.

4.4.5 **IT should form an integral part of the company’s risk management**

Chapter 2 Section 2.1 stated that IT forms an integral part of a company’s risk management and it is elaborated upon. Therefore the fifth requirement for IT governance requires that IT forms an integral part of the company’s risk management and for companies to comply with this requirement either of the following recommendations (PwC, 2015:1) should be stated in their annual reports:

- State that IT-related risks forms part of the company’s risk management activities and considerations.
- Indicate that the company complies with the IT-related laws, rules, codes and standards.
- Also state that the management of the company regularly report to the Board of Directors that the company has adequate business resilience arrangements in place for disaster recovery.

Graph 4.5 reveals the results of the fifth requirement that was gained through the evaluation of the top 40 JSE listed companies.
Graph 4.5: Results of the requirement stating that it should form an integral part of the company's risk management

Graph 4.5 clearly indicates that 24 of the 40 companies (60%) conform to the fifth requirement. Only 16 out of 40 companies (40%) of the top 40 JSE listed companies do not comply with the fifth requirement.

4.4.6 The Board of Directors should ensure that information assets are managed effectively

It is essential in IT governance that the management of the information assets by the Board of Directors is disclosed. In order for companies to comply with this requirement, any of the following recommendations should be stated in the company’s annual reports (KPMG, 2009:6):

- Indicate that formal procedures to manage information are in place which encompasses information security (protection of information).
- State that information is managed and personal information (information privacy) is protected.
- State that the Board of Directors ensures that an Information Security Management System is developed and implemented.
- State that the Board of Directors approve the information security strategy and delegates and empowers management to implement the strategy.

Along with all the suggested requirements mentioned above for the compliance with the sixth requirement, the graph below shows the results of the companies evaluated.

**Graph 4.6 Results of the requirement stating that the Board of Directors should ensure that information assets are managed effectively**

![Pie chart showing compliance and non-compliance](image)

Graph 4.6 illustrates the percentages of the results obtained in the evaluation, 16 out of the 40 companies (40%) comply with the sixth requirement while 24 out of the 40 companies (60%) do not comply with the requirement that states that the management of the information assets is the duty of the company’s Board of Directors.

**4.4.7 A risk committee and audit committee should assist the Board of Directors in carrying out its IT responsibilities**

The Board of Directors needs assistance for proper management of IT governance, therefore the risk committee and the audit committee needs to assist the Board of Directors in carrying out its responsibilities.
Either of the following suggested recommendations should appear in the company’s annual report in order to comply with this requirement (PwC 2015:1):

- It is stated that the risk committee ensures that IT-related risks are adequately addressed.
- State that the risk committee obtains appropriate assurance that controls are in place and are effective to address IT-related risks.
- State that the audit committee considers IT as the going concern of the company as it relates to financial reporting.
- Also indicate that the audit committee considers the use of technology to improve audit coverage and efficiency.

Graph 4.7 provides the results obtained from the analysis of the top 40 JSE listed companies to assess whether the companies comply with the last.

**Graph 4.7:** Results of the requirement stating that a risk committee and audit committee should assist the Board of Directors in carrying out its IT responsibilities

According to Graph 4.7, 22 of the 40 JSE listed companies (55%) are compliant to the requirement that the audit committee and the risk committee
should assist the Board of Directors in carrying out its duties. The remaining 18 of the 40 companies (40%) that were evaluated do not comply with the seventh requirement of the IT governance requirements.

4.4.8 Total compliance of the evaluated companies

Chapter 2 Section 2.4 claimed that IT governance is essential to the company’s corporate governance; therefore compliance with the King III IT governance disclosure requirements is important for good corporate governance.

Graph 4.8 indicate the percentage of the companies that fully comply with the IT governance requirements, the companies that partially comply and the companies that do not comply with any of the requirements.

Graph 4.8: Results of the compliance of IT governance requirements

Graph 4.8 indicates that 16 out of the 40 JSE listed companies (40%) are fully compliant to IT governance while 10 of the 40 companies (25%) partially comply, which means that the companies partially understand or misinterpreted the requirements of the King III report as is concluded in Chapter 2 that the report is not clear and can be misinterpreted. Furthermore, 14 out of the 40 companies (35%) do not comply with any of the IT
governance requirements and this could mean that the companies do not understand or fail to interpret the King III report’s IT governance requirements appropriately.

4.5 COMPREHENSIVE SUMMARY AND CONCLUSION

Chapter 4 dealt with the analysis of the top 40 JSE listed companies’ compliance with King III’s IT governance requirements. The main aim of this chapter is to evaluate the selected companies to gain an understanding of the extent to which the companies comply with King III’s requirements for IT governance. King III sets out seven requirements for IT governance. In the first, third and fourth requirement less than 50% of the evaluated companies complied indicating that the companies misinterpreted what this requirement entails. The second requirement shows that 52% of the evaluated companies understood and complied with this requirement. The fifth requirement indicated that 60% of the companies complied with it, thus only a lesser percentage of the companies did not understand this requirement.

Again in the sixth requirement there was a decline as only 40% of the companies complied; this indicates that a higher percentage of the companies did not understand or the companies misinterpreted the requirement. The results of the last requirement indicated that above 50% of the companies understood and complied with the last requirement 7. Only 40% of the companies fully understood and complied with all King III’s IT governance and disclosure requirements and 25% of the companies partially complied. The remaining 35% of the companies did not mention anything about IT governance.

Chapter 5 provides a full summary of the previous chapters and a brief description of how the objectives were achieved throughout the study.
CHAPTER 5
SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 INTRODUCTION

The main aim of this study is to evaluate the extent to which the top 40 JSE listed companies comply with the IT governance disclosure in accordance with King III. This study discussed the importance of IT governance in entities since IT currently plays an important role in the functioning of companies and the day-to-day managing of an entity.

As IT is one of the important components of the company it can cause company failure if not managed and governed properly. This can be caused by the IT-related risks that have evolved through the evolution of IT. The importance of proper IT governance arose with the benefits and risks of IT affecting the organisation as a whole. The requirements of governing IT should be understood for companies to properly govern IT. Therefore the purpose of this study is to evaluate the top 40 JSE listed companies in order to determine whether the companies understand or misinterpret the King III IT governance and disclosure requirements and also to evaluate to what extent King III needs to be clarified. The main objective of this study was achieved through the secondary objectives, which are as follows:

- Determine current IT governance disclosure requirements according to King III.
- Determine IT governance disclosure requirements according to the ISO’s, SOX and ISA 315.
- Evaluate the top 40 JSE listed companies to identify the extent to which they comply with the king III IT governance and disclosure requirements.
- Make recommendations to King III IT governance disclosure requirements, in accordance with ISO’s, SOX and ISA 315, to clarify disclosure requirements to South African companies that have to comply with King III.
The main objective of this chapter is to give an overall summary of the study, how the secondary objectives were achieved and also to provide recommendations of the study and draw an overall conclusion.

5.2 SUMMARY OF THE STUDY

The research question of this study was: to what extent does the top 40 JSE listed companies comply with the King III IT governance disclosure requirements? The primary and the secondary objectives outlined above are summarised to have an understanding of how they were achieved. This study was divided into five chapters whereby Chapter 1 was the introduction of the study and Chapter 2 was the literature review. In Chapter 2 most of the secondary objectives were achieved. Chapter 3 discussed the methodology followed in this study, Chapter 4 was the data analysis and findings and the Chapter 5 makes recommendations and draw a conclusion.

5.2.1 Chapter 1

Chapter 1 of this study provided the background and the problem statement. The problem that was identified in Chapter 1 is that the companies did not previously comply with King II IT governance and disclosure requirements. Therefore the evaluation of the top 40 JSE listed companies was necessary, which was done in Chapter 4. As previously confirmed it is important for companies to disclose and govern IT properly and to do so companies need to understand the IT governance and disclosure requirements set out in the King III report. Hence this study is important to help improve the King III report in developing comprehensive and easily interpretable IT governance and disclosure requirements. This will assist all companies that have to comply with the King III report.

Chapter 1 also outlined the primary and the secondary objectives of the study. A brief description of the methodology followed in the study, literature review, empirical review, target population, ethical considerations, measuring instruments and data collection methods were also highlighted in Chapter 1. Lastly Chapter 1 provided a chapter layout of the study.
The objectives and the problem statement that were outlined in Chapter 1 were discussed in Chapters 2 to 4.

5.2.2 Chapter 2

Chapter 2 was the literature review of the history of IT, risks, IT governance, different government regulations surrounding IT and the comparison between the King III report and the ISO’s, SOX, and ISA 315. In Chapter 2, a few secondary objectives were achieved as follows:

5.2.2.1 Determine current IT governance disclosure requirements according to King III

One of the secondary objectives that were set in the first chapter was to determine the current IT governance disclosure requirements according to the King III report. This was addressed and achieved in Chapter 2. King III is a report that is used to govern the South African companies on corporate governance. This report’s aim was to place South Africa at the forefront of governance internationally (Du Plessis, 2009:1). There are seven IT governance disclosure requirements set out by the King III report and these are as follows:

- The Board of Directors should be responsible for IT governance.
- IT should be aligned with the performance and sustainability objectives of the company.
- The Board of Directors should delegate to management the responsibility for the implementation of an IT governance framework.
- The Board of Directors should monitor and evaluate significant IT investments and expenditure.
- IT should form an integral part of the company’s risk management.
- The Board of Directors should ensure that information assets are managed effectively.
- A risk committee and audit committee should assist the Board of Directors in carrying out its IT responsibilities.
The requirements of IT governance and disclosure as set in King III were discussed and explained in depth in Chapter 2. The chapter also pointed out that the King III follows the apply or explain method. It was concluded that all companies are therefore required to apply these IT governance and disclosure requirements as set out, or declare why they are not complying.

Since IT is ever-changing and with the study that was conducted by Janse van Vuuren in 2006 based on the King II report showed that companies are not complying with the King report’s governance and disclosure requirements, it was ideal to do a study based on the King III report to evaluate whether the companies are now complying. Comparing King III with other international regulations (SOX, ISA 315 and ISO) was also ideal to find out where the report can be improved in order to assist companies’ compliance. This comparison formed part of the second secondary objective that was set.

5.2.2.2 Determine IT governance disclosure requirements according to the ISO’s, SOX and ISA 315 and compare them with King III

The second secondary objective that was identified was to determine IT governance disclosure requirements set according to the ISO’s, SOX and ISA 315 and to compare these regulations with King III. The three regulations were discussed in Section 2.5.2 to Section 2.5.4 of Chapter 2.

SOX

SOX is a regulation that was passed in the United States Congress, and this regulation is enforced on France, Germany, Italy and the USA, which also form part of the G8 countries. SOX consists of multiple sections that deal with different requirements of corporate governance, but only two sections address the IT governance and disclosure requirements: Section 302 and Section 404. These two sections were discussed in depth in Chapter 2 Section 2.5.2.

Section 302 did not specifically pin point the internal controls that the companies should disclose but it stated that companies should disclose all internal controls that adversely affect the issuer’s ability to record, process,
summarise, and report financial data and should identify and disclose any material weaknesses in internal controls. It was concluded that since Section 302 does not specify the internal controls to be disclosed, it can be deduced that a company’s computerised internal controls form part of IT governance and it should be disclosed because most organisations are using IT-based systems for the day-to-day activities of a company. Section 404 requires the companies to include the internal control report and again no specific requirements were addressed. It was concluded that no internal report can be complete without addressing IT governance.

**ISA 315**

ISA 315 is an international standard of auditing that is used in South Africa and in all the G8 countries and they have to comply with it since it was adopted by the European Union and the United Nations. The international standards were considered in this study to see to what extent the King III report differs from the IT governance and disclosure requirements required by this standard. Consideration of the international standards also assisted with formulating recommendations that the King III can apply to improve its report. The IT governance disclosure requirements set in ISA 315 are as follows:

- The auditor must assess if there are inconsistencies between the entity’s IT strategy and its business strategies.
- The auditor must assess changes in the IT environment and if there are installations of significant new IT systems related to financial reporting.

It was concluded that if the companies disclose IT governance, it can be regarded as a sign of good corporate governance.

**ISO**

ISO is an independent voluntary standard and any company can comply with it but it is not enforced in any country. According to the ISO the following should be disclosed in terms of IT governance disclosure:

- IT policies and objectives of the company in consideration of the strategic direction of the organisation should be disclosed.
• Establish an IT framework that clearly sets the objectives of the company out and which demonstrates the commitment of the company to meeting them.

• IT risk assessment analysis process that assesses the realistic likelihood and potential consequences of IT-related risks and has levels that rank the risks determined.

• Information about technical vulnerabilities should be obtained and ensure appropriate measures are taken to address the risks.

• The policies and agreements to maintain the security of IT is transferred within and outside the organisation.

After the requirements of the different regulations were identified and thoroughly explained in Chapter 2, King III’s IT governance and disclosure requirements were then compared to the IT governance and disclosure requirements of ISO, SOX and ISA 315. The comparison indicated that the King III report has some requirements that are similar to the other regulations and also had requirements that differ from ISO, SOX and ISA 315 and the outstanding differences should be added to the King III report to assist in improving the report so it can be clearly understood and interpreted.

5.2.2.3 Make recommendations to King III IT governance disclosure requirements, in accordance with ISO’s, SOX and ISA 315, to clarify disclosure requirements to South African companies that have to comply with King III.

Among the secondary objectives that was set in chapter one was to make recommendation to King III IT governance disclosure requirements, which are in accordance with ISO’s, SOX and ISA 315 to clarify disclosure requirements to the South African companies that have to comply with King III. This requirement is discussed in section 5.4 of this study.

5.2.3 Chapter 3

The aim of Chapter 3 was to provide a full description of the methodology followed in the study. It rendered an in depth explanation of research design,
research methodology, validity and reliability, data collection methods, ethical considerations, and data analysis.

The methodology that was used in this study was a mixed methodology, whereby the qualitative method was used in the literature review comparing King III against the selected international regulations (SOX, ISA 315 and ISO). The quantitative method was used to evaluate the top 40 JSE listed companies’ compliance with the King III IT governance and disclosure requirements.

Validity and reliability works differently depending on the methodology followed by the study. Since this study followed a mixed methodology it was determined that the validity and reliability of the study could not be measured in chapter 3. Therefore after the analysis that was conducted in chapter 4 of the top 40 JSE listed companies the results were obtained and it can be concluded that the study is valid and reliable because the measuring instruments and the measure are consistent. The same observation is repeatable and can still produce the similar results.

The population of the study was the top 40 JSE listed companies and all companies were selected for sampling (100 per cent sample). Chapter 3 also elaborated on the data analysis of this study which involved the evaluation of the top 40 JSE listed companies’ annual reports to find out if they mention or comply with any of the seven IT governance requirements. The methods that were used to analyse the data to be used in Chapter 4 was also discussed.

5.2.4 Chapter 4

The main objective of Chapter 4 was to provide data analysis and findings of the quantitative part of the study. The aim was to obtain an understanding as to whether the top 40 JSE listed companies understand or misinterpret the King III report’s IT governance and disclosure requirements and to evaluate whether there is a need for improving or elaborate the King III report. Chapter 4 also emphasised the third secondary objective that was set out in Chapter 1.
5.2.4.1 Identify to what extent the top 40 JSE listed companies comply with the above requirements and standards

This objective was achieved through the evaluation of the top 40 JSE listed companies’ annual reports. The evaluation was done through the comparison of the company’s annual report against the compliance requirements that were self-developed in Chapter 3 section 3.7. There are seven compliance requirements developed using the King III IT governance and disclosure requirements. The seven compliance requirements were tested against each company’s annual report in Table 4.1 and the results were as follows:

- Requirement 1: 53% of the companies were non-compliant and 47% were compliant
- Requirement 2: 48% of the companies were non-compliant and 52% were compliant
- Requirement 3: 58% of the companies were non-compliant and 42% were compliant
- Requirement 4: 58% of the companies were non-compliant and 42% of the companies were compliant
- Requirement 5: 40% of the companies were non-compliant and 60% of the companies were compliant
- Requirement 6: 60% of the companies were non-compliant and 40% of the companies were compliant
- Requirement 7: 45% of the companies were non-compliant and 55% of the companies were compliant

In conclusion of Chapter 4, the companies did not understand or rather misinterpreted the requirements of King III report regarding IT governance and disclosure because only 40% of the companies are fully compliant with the requirements while 25% of the companies partially complied and 35% did not mention anything about IT governance in their annual reports.
5.3 LIMITATIONS OF THE STUDY

Throughout this study the following limitations were identified:

- Lack of clarity as to why the companies are not disclosing IT governance.
- Lack of information on whether the companies are complying with IT governance or just not disclosing it in the company’s annual report.
- Not all of the top 40 JSE listed companies’ 2015 annual reports were available online.

The limitations identified in this study may have influenced the conclusions of the study. In Chapter 4 the lack of information as to why companies are not disclosing affected the conclusions. The companies could have been complying, but just not disclosing. In addition the lack of 2015 annual reports may also have influenced the conclusion because these companies may have disclosed IT governance requirements in their 2015 report. The limitations encountered in this study create opportunities for further research.

5.4 RECOMMENDATIONS

It can be concluded with the results obtained from this study that the King III report IT governance and disclosure requirements should be improved in order for the users to have a clear understanding. Some of the recommendations that are suggested for King III improvement or elaboration were obtained from the different regulations (ISO, SOX and ISA 315) that were compared with King III (in Section 2.5.1 to 2.5.4) in reference to the last secondary objective that was set in Chapter one are as follows:

- State that companies should establish safeguards to prevent data tampering (Correlog, 2011:2).
- State that companies should establish verifiable controls to track data access (Correlog, 2011:2).
- State that all companies should have an IT risk assessment analysis process which assesses the realistic likelihood and potential
consequences of IT-related risks and have levels that rank the risks determined (BSI, 2013:3).

- State that companies should disclose policies and agreements to maintain the security of IT and these policies should be transferred within and outside the organisation (BSI, 2013:3).

These recommendations can be implemented by the King III report to avoid non-compliance by companies with the IT governance disclosure requirements which may also enhance compliance.

5.5 SUMMARY AND CONCLUSION

IT plays a vital role in companies in this current environment, and therefore governance of IT is equally important. The South African companies that are listed on the JSE are supposed to comply with the King III report in terms of governance and disclosure.

The comparison of the different international regulations with King III was done to assess whether the King III is similar to other regulations. It was then identified that the report has some other requirements, thus an evaluation of a company’s annual reports was necessary in terms of the compliance of IT governance and disclosure requirements. The evaluation assisted to draw the conclusion that the King III report may not be easy to understand since most of the companies were not complying with the IT governance disclosure requirements.

It is important for companies to govern IT accordingly; hence this study was done to assist all companies to be able to achieve good corporate governance and increase awareness regarding the importance of IT governance. This was achieved by providing the King III report recommendations for IT governance disclosure requirements that it may be easily interpreted and understandable.

For further studies the researcher should consider all the JSE listed companies that are still not complying with IT governance and disclosure requirements to determine whether non-compliance is due to misinterpretation
of the King III requirements or whether there are other causes for non-compliance.
REFERENCE LIST


Anon. 2015. About ISO. http://www.iso.org/iso/home/about.htm Date of access: 29 Apr. 2015.


Brisebois, R., Boyd, G. & Shadid, Z. 2009. What is IT Governance? And why is it important for the IS auditor. Canada: INTO IT.


CLA (CliftonLarsonAllen). 2013. The role of internal audit in risk governance: How organisations are positioning the internal audit function to support their approach to risk management.


National Computing Centre. 2005. IT governance and developing a successful governance strategy: A best practice guide for decision making in IT. USA: NCC.


### APPENDIX A

**RESULTS OF IT GOVERNANCE DISCLOSURE TESTS DONE ON THE TOP 40 JSE LISTED COMPANIES**

**TESTS DONE AS PER CHAPTER 4, TABLE 4.1:**

<table>
<thead>
<tr>
<th>TEST</th>
<th>COMPLIANCE REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong></td>
<td>The Board of Directors should be responsible for IT governance.</td>
</tr>
<tr>
<td><strong>2.</strong></td>
<td>IT should be aligned with the performance and sustainability objectives of the company.</td>
</tr>
<tr>
<td><strong>3.</strong></td>
<td>The Board of Directors should delegate to management the responsibility to implement an IT governance framework.</td>
</tr>
<tr>
<td><strong>4.</strong></td>
<td>The Board of Directors should monitor and evaluate significant IT investments and expenditure.</td>
</tr>
<tr>
<td><strong>5.</strong></td>
<td>IT should form an integral part of the company’s risk management.</td>
</tr>
</tbody>
</table>
6. The Board of Directors should ensure that information assets are managed effectively.
   Is it disclosed in the company’s annual report that the Board of Directors ensures that information assets are managed effectively?

7. A risk committee and audit committee should assist the Board of Directors in carrying out its IT responsibilities.
   Is it disclosed in the company’s annual report that the risk committee and the audit committee assist the Board of Directors in carrying out its IT responsibilities?

<table>
<thead>
<tr>
<th>KEYS</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>√</td>
<td>The company <em>complies</em> with the IT governance requirement in its annual report.</td>
</tr>
<tr>
<td>X</td>
<td>The company <em>does not comply</em> with IT governance requirement in its annual report.</td>
</tr>
</tbody>
</table>

The results of the tests are as per table below. The numbers in the first row of the table below represent the requirements listed as per table above and correspond with the number in the table above.

<table>
<thead>
<tr>
<th>Company name</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company 1</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>None</td>
</tr>
<tr>
<td>Company 2</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>Fully</td>
</tr>
<tr>
<td>Company 3</td>
<td>√</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>√</td>
<td>Partially</td>
</tr>
<tr>
<td>Company name</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>Compliance</td>
</tr>
<tr>
<td>--------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>------------</td>
</tr>
<tr>
<td>Company 4</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Fully</td>
</tr>
<tr>
<td>Company 5</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Fully</td>
</tr>
<tr>
<td>Company 6</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>Partially</td>
</tr>
<tr>
<td>Company 7</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Fully</td>
</tr>
<tr>
<td>Company 8</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>Partially</td>
</tr>
<tr>
<td>Company 9</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>None</td>
</tr>
<tr>
<td>Company 10</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>None</td>
</tr>
<tr>
<td>Company 11</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Fully</td>
</tr>
<tr>
<td>Company 12</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>Partially</td>
</tr>
<tr>
<td>Company 13</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Fully</td>
</tr>
<tr>
<td>Company 14</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>Partially</td>
</tr>
<tr>
<td>Company 15</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>None</td>
</tr>
<tr>
<td>Company 16</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>None</td>
</tr>
<tr>
<td>Company 17</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Fully</td>
</tr>
<tr>
<td>Company 18</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>None</td>
</tr>
<tr>
<td>Company 19</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Fully</td>
</tr>
<tr>
<td>Company 20</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>None</td>
</tr>
<tr>
<td>Company 21</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>Partially</td>
</tr>
<tr>
<td>Company 22</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>Partially</td>
</tr>
<tr>
<td>Company 23</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>Partially</td>
</tr>
<tr>
<td>Company 24</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>Partially</td>
</tr>
<tr>
<td>Company 25</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>None</td>
</tr>
<tr>
<td>Company 26</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Fully</td>
</tr>
<tr>
<td>Company 27</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>None</td>
</tr>
<tr>
<td>Company 28</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Fully</td>
</tr>
<tr>
<td>Company name</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>Compliance</td>
</tr>
<tr>
<td>--------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>------------</td>
</tr>
<tr>
<td>Company 29</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>None</td>
</tr>
<tr>
<td>Company 30</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Fully</td>
</tr>
<tr>
<td>Company 31</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Fully</td>
</tr>
<tr>
<td>Company 32</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>None</td>
</tr>
<tr>
<td>Company 33</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Fully</td>
</tr>
<tr>
<td>Company 34</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>None</td>
</tr>
<tr>
<td>Company 35</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Partially</td>
</tr>
<tr>
<td>Company 36</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Fully</td>
</tr>
<tr>
<td>Company 37</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Fully</td>
</tr>
<tr>
<td>Company 38</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>None</td>
</tr>
<tr>
<td>Company 39</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Fully</td>
</tr>
<tr>
<td>Company 40</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>None</td>
</tr>
</tbody>
</table>

| TOTAL   | ✓ | 19 | 21 | 17 | 17 | 24 | 16 | 22 |
| TOTAL X  | 21 | 19 | 23 | 23 | 16 | 24 | 18 |
| TOTAL COMPANIES | 40 | 40 | 40 | 40 | 40 | 40 | 40 |

| Fully Compliant Companies | 16 |
| Partly Compliant Companies | 10 |
| Non-Compliant Companies     | 14 |