THE ROLE OF THE BOARD OF DIRECTORS IN IT GOVERNANCE

by

LYNDSAY RONALD MASEKO

MINOR DISSERTATION

Submitted in partial fulfilment of the requirements for the degree

MASTER'S COMMERCII

in

COMPUTER AUDITING

in the

FACULTY OF ECONOMIC AND FINANCIAL SCIENCES

at the

UNIVERSITY OF JOHANNESBURG

Supervisor: Professor Doctor B Marx

2015

ABSTRACT

Information technology (IT) is increasingly evolving to be crucial in the operation, support, sustainability and expansion of the modern organisation and should be managed as an important strategic asset that creates opportunities and provides a competitive edge. Embracing IT oversight as part of its fiduciary duties is indicative of the board's leadership, accountability and responsibility, which in turn demonstrates its foresight with regard to understanding the enormous impact IT has on strategic decision-making. However, owing to the complexity and general lack of understanding of IT, the management of IT is often treated as a separately managed value-providing asset and rarely receives the necessary attention of the board, thereby creating a disconnect between the board and IT. The result is that the board is not able to effectively fulfil its role in terms of IT governance. King III provides principles and recommended practices for effective IT governance in order to create a greater awareness at board level, but no detailed guidance is provided. Instead, numerous international guidelines are recommended to be used as frameworks to assist with the effective implementation of IT governance. COBIT 5 provides, as part of its governance process practices, related guidance activities linking it to the seven IT governance principles of King III, making it a practical framework to implement King III recommendations.

This research study sought to establish the extent to which the governance processes, practices and activities of COBIT 5 map to the recommended practices of IT governance as highlighted in King III. The objective of the study is to suggest to the board a possible "one-stop shop" to effective IT governance by means of adopting COBIT 5 as a framework for IT governance and by doing so, execute its duties in terms of IT governance. This was done via performing an extensive literature review on King III principles and recommended practices for effective IT governance as well as COBIT's governance domains and its activities and processes.

The study revealed that although King III principles and practices may be interpreted as vague with regards to *how* to implement IT governance principles, COBIT 5 bridges the gap between control requirements, technical issues, information systems and business risk to facilitate better governance of IT. The study also revealed that

COBIT 5 contains additional activities to assist the board in more transparent reporting of IT performance and conformance management to stakeholders as well as the need for connecting resource management with human resources and financial planning.

Keywords:

Board

IT Governance

King III

COBIT 5

Governance activities

ACKNOWLEDGEMENTS

I wish to acknowledge the support, patience and contributions made by the following individuals to the successful completion of this minor dissertation:

- God Almighty, without whom none of this would've been possible;
- My study leader, mentor and friend, Professor Ben Marx who believed in me when I at times didn't. You are truly a giant who allowed me to stand on your shoulders;
- My colleague and friend, Mafusi Lephoto for encouraging me and proof reading countless versions of this dissertation. I truly appreciate your valuable time and insightful remarks;
- My wife, Thembi, and our beautiful son, Qhayiya. Thank you for all the support, love and sacrifices made for this study to have come to fruition. You were my light when the tunnel seemed dark and lonely. Without you this achievement has no meaning.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE
INTRODUCTION AND STUDY LAYOUT

1.1. BACKGROUND

Since the release of the first King Report on Corporate Governance (known as "King I") in November 1994, the King Code of Governance for South Africa 2009 (hereafter referred to as "King III") for the first time, includes a chapter subscribing principles on how to achieve effective governance of information technology (IT) in entities. Supporting the inclusion of this new chapter, the committee stated in its introduction and background chapter that "information systems were used as enablers to business, but have now become pervasive in the sense that they are built into the strategy of the business. The pervasiveness of IT in business today mandates the governance of IT as a corporate imperative" (IoD, 2009:14). IT is an integral part of an organisation and is incorporated in all aspects of its business processes. It is increasingly evolving to be crucial in the operation, support, sustainability and expansion of the modern organisation and should be managed as an important strategic asset that creates opportunities and provides a competitive edge (Van Grembergen, De Haes & Guldentops 2004:2; IoD, 2009:14; Butler & Butler, 2010:33; Nel, 2011:4; Marnewick & Labuschagne, 2011:661; Ali & Green, 2012:179-180).

IT has transformed within the modern organisation. It is no longer playing the role of service provider but a more integral one: that of strategic partner (Van Grembergen, De Haes & Guldentops, 2004:2). IT strategy should therefore not only be aligned to business strategy but should be fused together with business strategy because IT strategy "transcends traditional functional areas such as marketing, procurement, logistics, operations and others", so that in due course no separation will exist between business strategy and IT strategy (Bharadwaj, El Sawy, Pavlou & Venkatraman (2013:472). As strategic partner and business enabler, it is difficult to distinguish IT from the organisational strategic mission, as it serves to increase the company's profits and shareholder value (Lainhart & John, 2000:33; Posthumus & von Solms, 2005:12; Ragphupathi 2007:95; Kaselowski, Von Solms & Von Solms, 2010:336).

Together with the strategic evolution of IT within the organisation, the *IT spending and staffing benchmark 2014/2015* survey found that IT executives increased IT

spending to a rate of 2.4% of revenue in 2013 and slightly decreased this in 2014 to 2.2%, which is indicative of significant investment made towards IT annually. Given the strategic partnership role IT fulfils within the organisation partnered with the significant investment made thereto, management must constantly be aware of the significant risks, vulnerabilities and challenges brought about by the use of IT and must ensure that these are governed and well managed (Posthumus & von Solms, 2005:11; IoD, 2009:15).

1.2. IT RISKS AND ASSOCIATED FINANCIAL LOSS

The literature reveals that the vulnerabilities, risks and challenges of organisations making extensive use of IT are those of unauthorised changes made to the IT systems, compromised confidential information, additional compliance burdens, loss of income due to disruption and poor functioning of the IT system, possible legal action against the organisation resultant from any of the aforementioned risk areas and unauthorised use of and access to the IT system and information (Gomes, 2007:11-13; Steenkamp, 2009:1; IoD, 2009:15).

Recent examples of unauthorised access to IT systems and their information and the resultant effect thereof were evidenced in incidents of cybercrime involving Sony Pictures Entertainment and Apple's iCloud through which terabytes of private information were obtained by hackers from mainframe computers (Lee, 2014, Rushton, 2014). South Africa also experienced a high-profile cybercrime incident when on New Year's Day 2012 a syndicate gained remote access to the Postbank's information systems. Media reported that the syndicate opened accounts across South Africa and after having gained access to two employees' computers, transferred cash between Postbank accounts and these accounts. Over the period 1 January 2012 to 3 January 2012, a total of R42 million was stolen from the bank (Chauke, 2012; Planting, 2012; Swart & Wa Afrika, 2012). Exacerbating the occurrence of this crime is the fact that it was committed three years after Postbank spent R15 million to upgrade its security systems.

Another IT failure which resulted in the loss of billions of Rands to the automotive industry was the poor implementation of eNaTIS (Van Reenen, 2007:39). The literature provides numerous other examples of cybercrime and IT failures that

resulted in huge financial losses being incurred (Parent & Reich, 2009:134; Ragphupathi, 2007:94):

- In 2001, Canada's second-largest grocery retailer, Sobeys Inc., abandoned an $89 million SAP implementation, taking an after-tax charge of $49.9 million, or $0.82 per share.
- Sydney Water, a public utilities company in Australia, abandoned a customer relationship management system and billing system in 2002, with an estimated write-off of AUD$61 million.
- In 2005, U.S. credential verification service provider ChoicePoint publicly admitted to inadvertently providing over 150 000 names, addresses and other sensitive information to criminals.
- American Express and Visa terminated their relationships with payment processor Cardsystems Solutions in 2005, whereby CardSystems improperly stored data which led to a data breach.
- Tokyo Stock Exchange had to suspend trade on many stocks in 2005, due to a vulnerability identified in its trading systems, being a lack of proper back-ups.

The board, tasked by King III with the responsibility of governing risk, ought to be keenly aware of the potential harms embedded in the organisations' value-creating activities and should be pro-active in showing leadership and strategic control in guiding efforts to meet risk management expectations (IoD, 2009:85; Weitzner & Peridis, 2011:34). These efforts should consist of the specific leadership, organisational structures and processes that ensure that the organisation's IT sustains and extends its strategy and objectives (De Haes and Van Grembergen, 2008). Attaining the aforementioned ensures effective governance of IT, which at its foundation requires an understanding of mitigating IT-related risks by means of IT security and other controls (Steenkamp, 2009:1).

Owing to the complexity of and the general lack of understanding, the management of IT is often treated as a separately managed "value providing asset" and rarely receives the necessary attention of the board. This creates what is "a basic

disconnect between boards and the IT" (Ragphupathi, 2007:95). The result of this disconnect is that many executives are intimidated by the task of managing technology because their mind set is that IT requires "special tools, special strategies and a special mind set" (Bensaou & Earl, 1998:120). One of the consequences of this is a misunderstanding of the value of effectively governing IT.

1.3. THE VALUE OF EFFECTIVE IT GOVERNANCE

IT in itself does not generate value. It is how IT resources are leveraged which ultimately results in IT's contribution to performance (Samuwai, Prasad, Green & Heales, 2012). In order to contribute to performance IT resources should be effectively governed by means of IT governance structures. This will ensure effectively managed IT resources, which in turn creates value for the organisation (Samuwai et al, 2012).

The value derived by an organisation from the effective governance of IT is wide-ranging and includes the following (Butler & Butler, 2010:33; Jianmu, 2007:4284 - 4285; Al Omari, Barnes & Pitman, 2012):

- Skilful mitigation of IT-related risks arising from threats to intellectual assets, information and IT in respect of availability, confidentiality and integrity of information assets.
- The provision of reasonable assurance that the organisation's IT processes are consistently delivering the efficiency gains for which they are designed.
- Achieving organisational critical success factors through the deployment of IT resources efficiently and effectively.
- Distinguishing developmental opportunities in pursuit of a competitive advantage through the way in which IT is used, thereby creating sustainable customer value and increasing company profits; and
- Compliance with evolving governance requirements such as King III and other regulatory and legal requirements such as increasing information and privacy related legislation.

The value add described above can however only be realised in an organisation where IT is governed effectively and at the correct level of management, where “IT governance is an integral part of effective corporate governance” (Steenkamp, 2009:1)

1.4. THE GOVERNANCE OF IT IN SOUTH AFRICA

According to Miles and Jones (2009:56), South Africa boasts a corporate governance regime comparable with most developed countries and a major influence on governance is the series of King reports. As Kaselowski, Von Solms and Von Solms (2010:336) assert, the King reports have no legal force, but are viewed as the de facto standard for good governance in South Africa. King III, released in September 2009, became operational on 1 March 2010, and introduced a few new concepts and principles. Key to this research study is the introduction of chapter five, which deals with the principles of the effective governance of IT together with the recommended practices to achieve such. This inclusion of IT governance in the code results in a governance code with more specific guidance in terms of IT-related strategies and controls, in comparison to previous codes. This in turn means that corporate governance goals are more readily achieved (Posthumus & Von Solms, 2005:13). This achievement of goals is attained via a more strategically aligned code of governance, with greater emphasis on internal controls and high level oversight, which should ensure greater accountability for IT failures from those charged with governance (Dhillon & Backhouse, 1996:74; Kaselowski, Von Solms & Von Solms, 2010:336, Khumalo, 2012:12).

The alignment of IT governance with corporate governance has proven to be problematic, as evidenced by the research findings of Chitambala (2006:34-35) on the status of IT governance in South Africa, which indicated that IT in South Africa, though identified as an important enabler of business, was not managed at the highest level of management. These findings correlate with the literature, which indicates that there is a disconnect in the modern organisation between the board and IT (Huff, Maher &. Munro, 2004:1; Valentine & Stewart, 2013:351-352). This disconnect can be ascribed to a general lack of adequate strategic skills and insights in IT, resulting in IT risks, with all its intricacies, not being fully understood and

effectively mitigated at board level (Posthumus & Von Solms, 2005:11; Posthumus, Von Solms & King, 2010:574).

King III aims to address these challenges via effectively governing IT by shifting the responsibility to top management, because those "boards who undertake the challenge of IT oversight, show that they understand the scope of their corporate accountability and responsibility, and are proactive in their leadership duties" (Posthumus & Von Solms, 2005:17). Hardy (2006:55) affirms that IT governance managed at board level results in effective oversight and alignment of IT with the overall business strategy of an organisation. In order to aid the board in executing prescribed principles of IT governance, King III recommends that the numerous international guidelines developed by various organisations such as ISACA, ISO and ITGI be used as frameworks to assist in the effective implementation of IT governance (IoD, 2009:15).

An additional hurdle to effective implementation of IT governance is the lack of a standard definition of IT governance. The term IT governance has rapidly advanced, and the literature provides many definitions thereof (Coertze & Van Solms, 2013:3359). The lack of a standard definition could result in ineffective measurement because that being measured might be measured in accordance with different interpretations of the definition. The aforementioned can be problematic: King III recommends that the board should follow an "apply or explain" approach when applying the principles of King III (IoD, 2009:5). The lack of a shared or standardised definition of IT governance could therefore result in a less than accurate result when an investor seeks to check the adherence of an organisation to the IT governance principles of King III by, for example, comparing two different entities' reports on applying the same principles. This is because the two boards may have different understandings of IT governance, and yet both organisations would claim to be adhering to the principles of King III.

Chapter three provides a detailed exploration of the different definitions of IT governance available in the literature, and, in addition to other definitions, provides a definition by Lee and Lee (2009:48) stating:

> *"IT governance is the clarification of decision-making rights and responsibilities as companies seek to leverage IT assets to business goals.*

This alignment is designed to allow organisations to achieve their goals through putting in place a systematic series of activities establishing structures and processes"

The definition above is adopted for the purposes of this dissertation.

The literature highlighted above forms the impetus to defining the research problem this study seeks to address.

1.5. THE BACKGROUND TO THE RESEARCH PROBLEM

IT is regarded as not only a technically difficult asset to manage in an organisation, but also as one that forms an integral part of the strategy of an organisation. It is moreover, something in which those charged with its governance have very little expertise (Damianides, 2005; Butler & Butler, 2010:34). Although boards recognise the value of IT to the organisation, it is often managed as a separate entity within the organisation and little to no attention is paid to the management of risk associated with the use thereof (Lainhart, 2000:21; Damianides, 2005:81; Parent & Reich, 2009:135). This often stems from a general lack of understanding by the board in terms of IT controls and a lack of technical insight required to manage IT in comparison to other strategic disciplines (Damianides, 2005:81; Butler & Butler, 2010:34). This opinion is supported by the findings of Marnewick and Labuschagne (2011:669), which indicate that though South African organisations adhere to corporate governance principles, very few adhere to the principles of IT governance due to a general lack of formal guidance. Indeed, Nolan and McFarlan (2005:2) assert that this lack of board oversight can be so dangerous that it puts the organisation at risk the same way that failing to audit the books would.

King III introduced principles to address this form of non-management of IT resources given the status of IT within the modern organisation. IT requires a proactive approach, and an understanding and management of IT-related risks (Raghupathi, 2007:96; Posthumus & Von Solms, 2005:17). IT governance is no longer solely the responsibility of IT personnel: corporate executives and boards have to become more involved to ensure that IT governance is correctly designed and implemented (Gomes, 2007:19; Reznik, 2007:57; IoD, 2009:15). Kordel (2002) agrees with this statement, asserting that:

- To derive full value from their IT investment and use of technology as a competitive weapon, organisations should make their business leaders accountable for the return on IT investments by putting them in charge of setting the IT agenda; and
- The most important factor distinguishing top-performing from substandard-performing organisations is the level of leadership by business and senior managers in a handful of key IT decisions.

Thoughtful and thorough IT governance is therefore paramount to the success of the modern organisation, because it is important that the board members of an organisation are fully equipped to accurately assess IT-related risks within their organisation's value-creating activities in order for them to have a meaningful voice (Raghupathi, 2007:95; Weitzner and Peridis, 2011:34).

King III therefore includes a chapter providing guidelines to the board relating to effectively governing this important strategic activity. The code however only provides principles and recommended practices to effective IT governance in order to create a greater awareness of IT governance at board level (IoD, 2009:15); no detailed guidance is provided.

Given this limited guidance provided in King III, as well as the apparent lack of board involvement in IT-related matters, the risk arises that board members may lack the fundamental knowledge needed to ask intelligent questions regarding IT governance. This will result in the delegation of IT governance to the Chief Information Officer (CIO) of the organisation and the governance of IT therefore being managed in an ad hoc manner (Nolan & McFarlan, 2005:1). This being the case, the boards' actions would circumvent the principle set by King III necessitating the involvement of the board in making IT-related decisions in order to foster a systematic and repeatable approach to desirable behaviour regarding IT decisions (Sandiro-Arndt, 2008).

The adoption of recognised frameworks of IT governance can assist those charged with governance to attain the advocated goal of effective IT governance. "Frameworks designate the structure of a set of objectives within a given domain, besides describing the relationships among those objects" (Lee & Lee, 2009:55). Differently stated, a framework is a real or conceptual structure intended to serve as

support or guide for the building of something that expands the structure into something useful (Kadam, 2012:25).

1.6. RESEARCH PROBLEM

Several formal and informal international guidelines and ISO standards have been developed over the years that can be used by organisations as a framework, roadmap, guide, template or sample to reflect that which was intended to be done was done, and to help management assess its effective implementation of IT governance (Symons, 2005; Chitambala, 2006:11; Gomes, 2007:27; IoD, 2009:15). In providing strategic direction and effective control over IT to achieve, sustain and enhance strategic objectives (IoD, 2009:82), the board must be aware of these frameworks available for their utilisation in achieving effective IT governance. Hardy (2006:56) contends that "board members need more specific guidance on how to achieve that vaunted goal of effective control." This guidance is required, because an effective board ensures that in terms of IT governance it is confident of where it is going, understands how to get there, is aware of what to expect along the way and knows when appropriate action needs to be taken (Afzali, Azmayandeh, Nassiri & Shabgahi. 2010:46). In addition to this, Steenkamp (2009:6) suggests that the adoption of a recognised framework for IT governance not only aids in the implementation of IT governance but also assists the organisation in the sense that it:

- Decreases cost because of the structured manner of implementation;
- Enhances the effectiveness of the end product, because frameworks are developed by many participants, which ensures that all aspects are covered; and
- Eases the assessment of compliance with external regulations.

King III however recognises that "no one size fits all" in terms of the IT governance due the variables such as size, utilisation of IT and the integration of IT into business processes (IoD, 2009:15), and it is therefore possible to adopt a combination of frameworks in order to achieve an effectively governed IT environment (Goeken & Alter, 2008:338)

The research problem therefore explored is that traditionally boards had little to no interest in IT-related issues, and yet they are confronted with a new hurdle in terms

of achieving effective corporate governance within the organisations via having to govern the unknown, being IT. It must be stated that boards recognise the importance and value of IT and in some instances would like to be more actively involved in their oversight thereof, but they often lack direction in terms of where to begin and how to proceed (Coertze & Van Solms, 2014:4426). This lack of direction can be partially solved by the effective implementation of a recognised IT governance framework or International Standards Organisation (ISO) best practice. Although there is no single framework currently that addresses all the requirements for effective IT governance, several frameworks do exist that are complementary, with strengths in different areas; this results in a "mix and match" approach often being adopted (Khanyile & Abdullah, n.d.).

The Control Objectives for Information and Related Technology ("COBIT") is widely considered as "the de facto standard for IT governance worldwide" (Marnewick & Labuschagne, 2011:668). Now in its fifth edition, it considers itself the framework to be adopted for enterprise-wide governance of IT. COBIT was designed to bridge the gap between technical people and business people by facilitating a common understanding of IT (Kadam, 2012:21). COBIT 5 was released in April 2012 as a framework to govern enterprise IT in a holistic manner to cater for end-to-end business and IT functional areas (De Haes, Van Grembergen & Debreceny, 2013:307). In order to achieve an end-to-end holistic governance framework, COBIT 5 differentiates between IT management and the governance of IT to allow for better decision-making (Kadam, 2012:25). COBIT 5 also integrates frameworks such as COBIT 4.1., Val IT, Risk IT as well as concepts from Business Model for Information in order to provide a one-stop solution to the governance of IT (Khanyile & Abdullah, n.d.). COBIT 5 also aligns itself at a high level with existing frameworks such as ITIL, TOGAF, PMBOK, PRINCE 2 and ISO in order to form an umbrella framework to IT governance (Kadam, 2012:21–22; Khanyile & Abdullah, n.d., De Haes, et al., 2013:319). Of critical importance to this research study is that COBIT 5 provides, as part of its governance process practices, related guidance activities linking it to the seven IT governance principles of King III. This makes it the most practical framework linked to King III recommendations.

This research study seeks to establish the extent to which the governance processes, practices and activities of COBIT 5 conform to the recommended

practices of IT governance as highlighted in King III. This study will make a contribution to the literature, as it will provide a detailed mapping of each recommended principle and practice of King III, to the governance processes, practices and activities of COBIT 5.

The research problem:

To establish the extent to which COBIT 5 can be utilised by the board as a framework to achieve the IT governance principles set out in King III.

1.7. AIM AND OBJECTIVES OF THE STUDY

The aim of this research study is to establish the extent to which COBIT 5 can be used as a framework of enterprise IT governance in order to assist the board of directors to effectively apply the principles of King III, resulting in effective IT governance. In order to achieve the aim of this study, the following objectives must be met:

- To identify the recommended principles and practices of King III with regard to the effective governance of IT.
- To highlight the evolution of COBIT to illustrate the main prescriptive differences.
- To establish the governance domain prescribed by COBIT 5 framework for effective IT governance by the board via evaluate, direct and monitor practices.
- To map the recommended practices of King III to the governance processes, practices and activities of COBIT 5.
- To identify possible shortcomings within the COBIT 5 framework when compared to King III; these the board of directors would need to address in order to mitigate resultant risks.

The objectives of this study will be achieved by means of performing a literature review (chapters 2 to 4) of; corporate governance in South Africa, with a specific focus on the introduction of IT into the King Codes, the development of IT governance and its resultant impact on the board of directors and how COBIT can be utilised as a framework for IT governance. The methodology adopted, findings and

conclusions with regard to the mapping of King III to COBIT 5 will be discussed in chapter 5.

COBIT 5 was selected as the preferred framework because (Hardy, 2006:59-60; IoD, 2009:15; Steenkamp, 2009:7; Kadam, 2012:21-22; De Haes, et al., 2013:319; Khanyile & Abdullah, n.d.):

- King III makes specific mention of COBIT;
- Research indicates that COBIT is widely used adopted by organisations;
- The framework is freely downloadable;
- It is viewed as the generally accepted standard for IT governance;
- COBIT 5 provides a framework which integrates existing frameworks;
- COBIT 5 provides a holistic view of the enterprise, covering both business and IT from end-to-end; and
- COBIT provides a sound approach to implementing IT governance-related initiatives in a well-controlled environment.

1.8. STUDY LAYOUT

The research study is divided into the following chapters:

Chapter 1: Introduction

The background to the research problem is discussed. The study layout to be followed to support the research findings in order to meet the set objectives is discussed in detail.

Chapter 2: The development of corporate governance in South Africa

This chapter deals with a literature review on the development of corporate governance in South Africa with a specific focus on the basis for the inclusion of chapter five in King III.

Chapter 3: Conceptualising IT governance

The concept IT governance is explored, and a standardised definition for the purpose of this research study is reaffirmed. A link is also established between corporate governance and IT governance within the broader enterprise governance concept.

Chapter 4: COBIT as an effective IT governance tool

In this chapter, the origins and background to the development of COBIT will be briefly discussed. The major changes evident through the evolution of the framework will also be explained, and why COBIT is an effective IT governance tool will be explored.

Chapter 5: Research methodology and research findings

In this chapter, the principles for effective governance as recommended in King III are compared to the governance domain of COBIT 5. The findings of the comparison are also explained and discussed.

Chapter 6: Conclusion

In this chapter the objectives of the research study are concluded upon and areas for further research areas identified.

1.9. CONCLUSION

In this chapter, the importance of IT in the modern organisation was delineated. The value of IT was explored, and, with it, the resultant risks that accompany IT if not managed at the appropriate level and with the necessary buy-in from top management. The chapter also referred to the importance of King III principles for the effective governance of IT and the impact thereof on traditional boards who may not be adequately equipped with the skills and expertise to deal with these requirements. The background to the research problem was sketched and the existence of the de facto standard in IT governance, COBIT, was introduced as a possible facilitator of effective governance. In order to exercise effective oversight over IT, the role of board includes the identification of relevant frameworks for effective implementation of IT governance. For the purposes of this research study, COBIT was selected.

In the next chapter, the development of corporate governance in South Africa will be discussed as well as the emergence of IT governance through the Codes of Governance in South Africa.

CHAPTER TWO

DEVELOPMENT OF CORPORATE GOVERNANCE IN SOUTH AFRICA

2.1. INTRODUCTION

Globally, the subject of corporate governance has received increased attention due to corporate scandals resulting in amendments to legislation such as Sarbanes-Oxley Act (SOX) and the Companies Act no. 71 of 2008 in order to more effectively manage relationships between organisations and stakeholders (Vaughn & Ryan, 2006:504; Gomes, 2007:14, IoD, 2009:4; Ntim, Opong, Danbolt & Thomas, 2012:122). The human condition, which is characterised by self-interest and opportunism, necessitates corporate governance to ensure that those in a position of trust act in the best interests of all stakeholders (Mostovicz, Kakabadse & Kakabadse, 2010:614; Mahadeo, Soobaroyen & Hanuman, 2012:339).

The board, tasked with determining the strategic direction of an organisation, has an operational responsibility towards the stakeholders to ensure that the business continues in the face of system failures, threats and attacks (Andriole, 2009:374). These responsibilities fall within the ambit of the broad framework of enterprise governance (Motloutsi, 2009:11); hence any management approach that is governance-conscious must seek to synchronise business and IT (ISACA, 2012).

Good governance, which is a characteristic of effective leadership (IoD, 2009:19), sets the boundaries of accepted behaviour for both organisations and societies. It is pluralistic in nature, also in the sphere of decision-making, it empowers the weak in societies and achieves the common good (Kakabadse & Korac-Kakabadse, 2002:305). Well-governed organisations are so valuable that investors in emerging countries such as South Africa are willing to pay a premium for their shares (Vaughn & Ryan, 2006:504). The willingness to pay this premium and the need for a set of boundaries are necessitated by, among other things, the existence of the agency problem.

2.2. THE AGENCY PROBLEM

The agency problem arises where the owners of companies no longer control their own interests and this control is delegated to the managers of the company – i.e. the

directors. The result could be the abuse of power by managers for self-interest at the expense of the owners of the company (Rossouw, Van der Watt & Malan, 2002:289; Marx, 2008:93; Schooley, Renner and Allen, 2010:152). The agency problem, however, takes a myopic view in terms of governance and has been criticised for its narrowness in term of governance (Kyereboah-Coleman, 2007:20-21). Aguilera, Filatotchev, Gospel and Jackson (2008:475) described the agency problem as a closed system which devotes little attention to the distinct contexts within which an organisation operates. A more recent emphasis on governance has been a gradual move away from the more centric investor / agency problem approach, to a more inclusive stakeholder orientated approach (Brennan, Niamh & Solomon, 2008:890).

2.3. THE STAKEHOLDER THEORY

The stakeholder theory originates from the view that all stakeholders have intrinsic interest and hence the organisation has the responsibility to all its stakeholders that it affects or that affect its decision-making (Kyereboah-Coleman, 2007:22; Alpaslan, Green & Mitroff, 2009:8). According to this theory, no one's interests therefore dominate over those of others. The stakeholder theory of governance was popularised by the first two King Reports (Brennan, Niamh and Solomon, 2008:890) and has its roots in the stakeholder theory of Edward Freeman (West, 2009:13).

The stakeholder theory overcomes the agency problem, as it is a more inclusive theory which establishes a set of relations and mechanisms that guide the board of directors to act in a manner that is good for the providers of capital, the management and the stakeholders at large (Nikolic & Eric, 2011:69). These relations and mechanisms can be described as corporate governance, which if effectively implemented can result in an improvement in transparency and accountability (Bajo, Bigelli, Hillier & Petracci, 2008:2; Mahadeo, Soobaroyen & Hanuman, 2012:339). To better understand these relations, mechanisms and existing boundaries associated with effective governance, the concept corporate governance must be defined.

2.4. DEFINING CORPORATE GOVERNANCE

In the literature various definitions of corporate governance are found, such as:

> *Focussing "mainly on the systems by which companies are directed and controlled. It is a collection of law and practices, grounded in the fiduciary*

duties and their application regulates the conduct of those in control" Aka (2007:238)

The "processes and procedures that act as the boundaries of accepted behaviour for both the organisations and societies, as well as, if appropriately applied, an opportunity – creating environment" Kakabadse and Korac-Kakabadse (2002:305)

The relationships between corporate managers, directors and stakeholders. It can also encompass the relationship of the corporation to the stakeholders and society. Corporate governance can encompass the combination of laws, regulation, listing rules and voluntary private sectors practices that enable the corporations to attract capital, perform efficiently, generate profit and meet both legal obligations and general societal expectations. (Gregory and Simms, 1999)

"The set of mechanisms – both institutional and market-based – that induce the self-interested controllers of a company (those that make decision as to how the company will be operated), to make decision that maximises the value of the company to its owners (the suppliers of capital)" (Denis & McConnel, 2002:1).

The corporate governance definitions listed above can be categorised into narrow and wide definitions. In the literature (Rossouw, 2009:38; Corina & Roxana, 2011:675; Gavrea & Stegerean, 2011:92-93; Shapatoti, 2011, Yasser, 2011:204) the classifications are described as follows:

- The narrow definition describes the relationship among various participants in order to determine the direction of an organisation, and
- The wider definition of corporate governance is the practice through which an organisation is directed and controlled by means of laws, regulations, listing rules and voluntary practice.

Irrespective of how corporate governance is defined or whether a narrow or broad definition is adopted, corporate governance "affects the economic stability and growth prospects of a country" (Vaughn & Ryan, 2006:504). South Africa, Africa's second largest and most sophisticated economy is no different in this regard.

Summative comment

The prominence of corporate governance gained traction following worldwide corporate collapses that in many cases can be ascribed to the existence of the agency problem in management. Although it can be broadly defined, the substance of all definitions of corporate governance can be reduced to either the narrow definition of purely a focus on organisational stakeholding or the wider definition, which requires cognisance of the laws and regulations governing the organisation. The corporate governance regime of South Africa is a blend of these views.

2.5. CORPORATE GOVERNANCE IN SOUTH AFRICA

"South Africa boasts a corporate governance regime comparable with the most developed economies" in the world (Miles & Jones, 2009:56). It has been described as "world class" (West, 2006:437), and ranks in the top decile of emerging market countries' corporate governance frameworks (IIF, 2007:11). The need for a top class code of corporate governance was necessitated by the post-apartheid era, when significant foreign investment flowed to South Africa and a robust foreign market criticising the corporate structure in the country and in turn demanding corporate reform in South Africa (Aka, 2007:242; Marx, 2008:203; Miles & Jones, 2009:56). These forces of change drove a move towards the establishment of standardised governance in corporate South Africa, the result being the King Report on Corporate Governance and the Code of Corporate Practices and Conduct also known as "King I".

2.5.1 The King report on Corporate Governance and the Code of Corporate practices and Conduct, 1994 (King I)

Rising from economic isolation and a change in the political landscape post the 1994 elections, South Africa faced the challenge of developing a code of governance that would not only assist it in participating in the global economy (via attracting direct foreign investment into the country), but would also ensure its allegiance to the South African people affected by apartheid. The first King Report was published on 29 November 1994 with an effective implementation date for reporting in respect of years commencing after 30 June 1995. King I was an initiative from the Institute of Directors of South Africa (IoD) to develop a code of governance and corporate

practice for South Africa (Marx, 2008:206) with the primary objective of achieving the highest standards of corporate governance by using an integrated approach (Vaughn & Ryan, 2006:506). An integrated approach to governance encompasses an approach through which companies recognise that they do not operate independently from the communities and societies within which they operate, and therefore advocates that principles of good governance must include good social, ethical and environmental practices (Aka, 2007:249-250).

The code consisted of four chapters that provided guidance on issues such as the board of directors (Section 2), the chairman (Section 3), non-executive directors (Section 4), directors' appointments (Section 5), directors' remuneration (Section 6), board meetings (Section 7), professional advice (Section 8), stakeholder communication (Section 9), auditing (Section 10), workers' participation (Section 11), affirmative action (Section 12) and a code of ethics (Section 13).

Some of the shortfalls of King I highlighted by Marx (2008: 206–207) included:

- It followed a 'tick-box' approach to compliance,
- It emphasised disclosure rather than focusing on best practice as its main incentive;
- It protected the vested interests of corporate groups in the South African economy; and
- It did not consult widely, did not invite public debate and did not draw on external expertise – and therefore avoided direct involvement in issues of corporate governance.

In addition to the above, Kakabadse and Korac-Kakabadse (2002: 307–309) identified the following deficiencies with regard to the implementation of King I in organisations:

- *Transparency:* Transparency and segmental disclosure appeared to be absent in most SA corporations, with possibly only the top 30–40 companies introducing certain performance measures. Generally, investors were considered to have been given inadequate information to assess the performance of individual units.

- *Interest of directors:* Directors' dealings were difficult to monitor and track. Despite the fact that insider trading investigations were on the increase, few cases were brought to prosecution.
- *Ownership:* The nature of nominee shareholding accounts made it difficult to trace ownership.
- *Family interest and controls:* Family control was often been exercised through various pyramid structures, which resulted in inappropriate governance and controls being applied on behalf of business.
- *Non-executive director (NED) agendas:* Certain NEDs represented majority shareholders or the parent company, whose interests were not aligned with those of other shareholders. The dominance of such critical shareholders was considered, on certain occasions, to override the interest of other shareholders.

A further noticeable absence from the code was that it did not make mention of IT governance. This is understandable, however, as, at the time, IT was used in business, but more as an enabler of business rather than a strategic partner, and hence was not yet a topical issue worth addressing in much detail.

Coupled with the above critique against what started out as a world class code, the need for revision was fuelled by an era plagued with international and local corporate scandals such as Leisurenet, MacMed and Regal Treasury Bank, to mention but a few, which necessitated the IoD to review King I in line with local concerns and global developments.

2.5.2 The King II Report on Corporate Governance and the Code of Corporate Practices and Conduct, 2002 (King II)

Following global and domestic developments in the sophistication of corporate governance worldwide tied with corporate collapses both internationally and domestically, the IoD committed itself to:

- a review of the currency of King I,
- an extension of the inclusive approach, and
- a consideration of risk and controls and recommendations for enforcement.

This would form part of the mandate given to chair of the committee, Mervyn King (West, 2006:435-436; Ntim, Opong, Danbolt & Thomas, 2012:125).

Given that South Africa is a developing country, the committee needed not only to consider issues surrounding "corporate collapses and creative accounting; the driving force behind corporate governance reforms, but they had to also consider the effects on economic development and of globalisation and balance a locally acceptable and relevant corporate governance strategy with the need to meet international expectation" (West, 2006:435). The approach adopted by the committee was that of using King I as a base and expanding on some of the issues raised by concerned stakeholders. Linking with a new approach to governance, the committee established and clearly defined what it believed was the underlying principles of good governance – discipline, transparency, independence, accountability, fairness and social responsibility – and further developed and integrated these fundamental principles into tangible guidelines for minimum standards of corporate governance (Vaughn & Ryan, 2006:506).

King II was issued in 2002 with an effective implementation date of 1 March 2002. It was a more principle-based code than King I, had the distinctive feature of placing more attention on non-financial corporate governance, expanded on the inclusive approach and shifted away from single bottom line reporting to triple bottom line reporting (Aka, 2007:250; Marx, 2008:208; West 2009:12; Diamond & Price, 2012:62). The report also unashamedly shared the philosophy of the Cadbury Report in the sense that it was not prescriptive but rather proposed a code of conduct to be voluntarily applied and self-policed (Kakabadse & Korac-Kakabadse, 2002:310). In an effort to overcome some of the criticism levelled against King I, the committee consulted extensively and collaborated "closely with the IoD in the UK and drew much from the Blue Ribbon and other US reports" (Kakabadse & Korac-Kakabadse, 2002:310); it also consulted Australian documents. In total the committee consulted some 103 documents and 44 websites all addressing the Anglo-American perspectives of corporate governance.

The result of all the above efforts was that the code now consisted of sections providing guidance on board of directors (section 2), risk management (section 3), internal audit (section 4), integrated sustainability reporting (section 5), accounting

and auditing (section 6), relationships with owners (section 7), communication (section 8) and implementation of the code (section 9) (Marx, 2008:211).

The report was hailed a notable example of devising unique solutions to align corporate governance with international best practice, while addressing corporate responsibility (Andreasson, 2011:655). Although labelled world class for its emphasis on social, environmental and ethical concerns (West, 2006:437), the main criticism levelled against King II was its self-regulatory nature as well as the lack of enforcement via statutory channels (Kakabadse & Korac-Kakabadse, 2002:311; Marx, 2008:214).

In King II mention was made of IT, but mainly in the form of acknowledging the risks associated with its use and how it could be better utilised within the organisation. No further detail was provided on the management of these risks as well as with whom the responsibility for the governance of IT should reside.

2.5.3 The King Code of Governance for South Africa and the King Report on Governance for South Africa, 2009 (King III)

The third report on corporate governance in South Africa became necessary due to the advent of the new Companies Act no. 71 of 2008 and changes in international governance trends (IoD, 2009:4). The committee for King III focused on the "importance of conducting business reporting annually in an integrated manner" – i.e. putting the results in perspective by also reporting on:

- how a company has, both positively and negatively, impacted on the economic life of the community in which it operated during the year under review; and
- how the company intends to enhance those positive aspects and eradicate or ameliorate the negative aspects in the year ahead (Gstraunthaler, 2010:148).

Unlike King I and II, King III was applicable to all entities irrespective of size and whether or not they were listed. The "apply or explain" basis of the King III report required every entity to apply the King III principles as best it could in meeting the objectives of the entity concerned (Butler & Butler, 2010:33-34).

The King III Report consists of nine chapters:

- Ethical leadership and corporate citizenship (Chapter 1)

- Boards and Committees (Chapter 2)
- Audit Committees (Chapter 3)
- The governance of risk (Chapter 4)
- The governance of information technology (Chapter 5)
- Compliance with laws, rules, codes and standards (Chapter 6)
- Internal audit (Chapter 7)
- Governing stakeholder relationships (Chapter 8)
- Integrated reporting and disclosure (Chapter 9)

Among the new trends and issues incorporated into the report were alternative dispute resolution, risk-based internal audit, business rescue, fundamental and affected transactions and an expansion on mention made of IT in King II, which resulted in the inclusion of a chapter on IT governance.

IT is essential to manage the transactions, information and knowledge necessary to initiate and sustain a company. “It has becomes increasingly difficult to distinguish organisational strategic mission from the IT that enables the mission …” (Raghupathi, 2007:95), and this provides more impetus for the inclusion of IT governance at the board level, as now recommended by King III.

Summative comment

As South Africa matured in its democracy and evolved into a world-class African country from economic sanctions in the early 1980s, it was imperative for corporate governance to keep evolving together with the changing economic landscape of the country. The King Code, the de facto standard for corporate governance in South Africa, developed from initially trying to promote the highest standards of corporate governance in South Africa by advocating an inclusive approach to governance, to already making brief mention of the growing importance of IT and globalisation in the second report issued in 2002. In King III, the committee identified the importance of IT within the modern organisation as having evolved from an enabler of business to being a key strategic asset and thus requiring board level attention at organisational level.

2.6. IT GOVERNANCE IN TERMS OF KING III

The ease of transacting via the internet, continued growth within e-commerce and increased on-line trading ensures that the modern organisation trades more efficiently, instantly. These competitive advantages brought about by a more expansive use of IT inherently increase the risk of IT to the organisation and require it to be controlled and governed at the highest level of management (IoD, 2009:15).

Chapter 5 of King III Report and section 5 of the code deal with the governance of IT. King III provides top management with a chapter outlining seven guiding principles behind IT governance, and these are supported by 24 recommended practices. A summary of the principles together with the recommended practices for each principle is provided in Table 2.1 below.

It is worth mentioning that in its introductory chapter to the code, the committee highlighted that "due to the broad and ever evolving nature of the discipline of IT governance, the chapter does not try to be the definitive text on the subject, but rather to create a greater awareness at director level" (IoD, 2009:15). This statement provides credibility to Botha (2014:13), who declares that while the code provides the board with *who* the responsibility of IT governance resides with as well as *what* should be done, the code does not outline *how* this should be done, which provides a further motivation for this study.

TABLE 2.1 Summary of IT governance principles and recommended practices per King III

IT Governance Principle	Recommended practice
5.1. The board should be responsible for IT Governance	5.1.1. The board should assume responsibility for the governance of IT and place it on the board agenda
	5.1.2. The board should ensure that an IT charter and policies are established and implemented
	5.1.3. The board should ensure promotion of an ethical culture and awareness a common IT language
	5.1.4. The board should ensure than an IT internal control framework is adopted and

	implemented
	5.1.5. The board should receive assurance on the effectiveness of the IT internal controls.
5.2. IT should be aligned with the performance and sustainability objectives of the company	5.2.1 The board should ensure that the IT strategy is integrated with the company's strategic objectives and business processes.
	5.2.2. The board should ensure that there is a process to identify and exploit opportunities to improve the performance and sustainability of the company through the use of IT.
5.3. The board should delegate to management the responsibility for the implementation of an IT governance framework	5.3.1. Management should be responsible for the implementation of the structures, processes and mechanisms for the IT governance framework.
	5.3.2. The board may appoint an IT steering committee of similar function to assist with its IT governance
	5.3.3. The CEO should appoint a CIO responsible for the management of IT.
	5.3.4. The CIO should be a suitably qualified and experienced person who should have access to and interact regularly on strategic IT matters with the board and/or appropriate board committee and executive management.
5.4. The board should monitor and evaluate significant IT investments and expenditure	5.4.1. The board should oversee the value delivery of IT and monitor the return on investment from significant IT projects.
	5.4.2. The board should ensure that intellectual property contained in information systems is protected.
	5.4.3. The board should obtain independent assurance on the IT governance and controls supporting outsourced IT services.
	5.5.1 Management should regularly demonstrate to the board that the company

5.5. IT should form an integral part of the company's risk management	has adequate resilience arrangements in place for disaster recovery.
	5.5.2. The board should ensure that the company complies with IT laws and that IT-related rules, codes are considered.
5.6. The board should ensure information assets are managed effectively	5.6.1. The board should ensure that there is a system in place for the management of information, including information security, information management and information privacy
	5.6.2. The board should ensure that all personal information is treated by the company as an important business asset and identified.
	5.6.3. The board should ensure that an Information Security Management system is developed and implemented.
	5.6.4. The board should approve the information security strategy and delegate and empower management to implement the strategy.
5.7. A risk committee and audit committee should assist the board in carrying out its IT responsibilities	5.7.1. The risk committee should ensure that IT risks are adequately addressed.
	5.7.2. The risk committee should obtain appropriate assurance that controls are in place and effective in addressing IT risks.
	5.7.3. The audit committee should consider IT as it relates to financial reporting and the going concern of the company.
	5.7.4. The audit committee should also consider the use of technology to improve audit coverage and efficiency.

Source: IoD (2009: 39-41)

2.7. CRITICAL LINK TO THE STUDY

Understanding the importance of the role IT fulfils within the modern organisation assists in understanding the need for it to be governed at the highest level as recommended by King III. The value derived from the use of IT within the organisation should however not be measured solely by the benefits without careful consideration being given to the inherent risk associated with the more extensive use of IT. This risk should be controlled and governed at the highest level of management – the board. The board, burdened with this responsibility, however, does not receive clear guidance in terms of how to execute its duties in relation to IT governance. This study endeavours to explore means to assist the board in discharging its responsibility towards IT governance in the most efficient and effective manner.

2.8. CONCLUSION

In this chapter the development of corporate governance under a changing economic landscape in South Africa was discussed. The human condition of self-interest and opportunism was highlighted as providing the impetus for the development of corporate governance. Evident from this chapter was that, although labelled world class, King I and II did not pay sufficient attention to the ever-growing dependence of the modern organisation on technology, but this was justifiable given when these codes were released. It is worth mentioning that even though not a lot of attention was given to IT in both these codes, King II already identified the dependence relationship that started developing between organisations and IT, possible competitive advantages to be derived therefrom as well as the associated risks resulting from extensive use thereof. King III expanded on this observation made in King II, highlighting the depth of the modern organisation's dependency upon IT and the need for it to now be managed at the highest level within the organisation as a strategic asset. IT governance in terms of King III was also discussed, bringing to the fore the fact that although principles are ascribed and recommended practices suggested, the board is left not necessarily understanding how to implement effective IT governance.

From being traditionally viewed as an enabler of business and as a separately managed asset apart from strategic governance decisions IT now needs to be addressed as a standing agenda point by the board. Recommending the board be responsible for IT governance now requires answers to questions such as:

- What is IT governance?
- Why is IT governance the responsibility of the board?
- What needs to be done in order to ensure the effective governance of IT?
- How does the literature link with the recommendations of King?
- Is there a fundamental difference between the management and governance of IT?

The next chapter will provide a detailed analysis of the above questions in order to equip those charged with the governance of an organisation to be aware of their responsibilities regarding IT governance.

CHAPTER THREE

CONCEPTUALISING IT GOVERNANCE

3.1. INTRODUCTION

As was evident from Chapter 2, the King III Code now recommends the incorporation of IT as strategic objective to be governed at the highest level. Factors motivating a higher-level management of IT include the spread and predominance of the internet, e-commerce, the creation of multinational organisations, the collaboration of organisations of different nations and the globalisation of economies (Chalaris, Lemos and Chalaris, 2005:59, IoD, 2009:15). All these factors contribute considerably to the establishment of IT governance as a subject of considerable importance within the modern organisation. The effective governance of IT within the modern organisation has in fact become so essential that it has "ultimately become the great wall separating enterprise success from enterprise failure" (McDonnell, 2006:54). To attain success, organisations must integrate information technology with business strategies to reach their business objectives and realise value from their information (Lainhart & John, 2000:33). In order to achieve this, effective IT governance linkage is required between the organisation's IT objectives and its business objectives, resulting in more results-driven actions (Reznik, 2007:57).

This chapter will focus on the concept IT governance, its key focus areas, why IT governance is the responsibility of the board, the processes required for effective IT governance, the linkage between the theory of IT governance and King III principles and understanding the differences between IT management and IT governance.

3.2. DEFINING IT GOVERNANCE

No standard definition of IT governance exists in the literature (Lee & Lee, 2009:47, Simonsson & Johnson, 2006). IT governance is therefore broadly defined and tends to be ambiguous at times. For the purpose of this study, meaning must be attached to the discipline and various definitions will be examined in order to establish such.

The literature defines IT governance as:

> "Specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT" (Weill & Woodham, 2003)

"… an organisational structure and set of processes that manage and control the enterprise's IT activities to achieve the enterprise's goals by adding value while balancing risk versus return over IT." (Kordel, 2002)

"... the organisational capacity exercised by the board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure fusion of business and IT." (Van Grembergen, De Haes & Guldentops, 2004:5)

"... the strategic alignment of IT with the business such that maximum business value is achieved through the development and maintenance of effective IT control and accountability, performance management and risk management" (Webb, Pollard & Ridley, 2006)

"...IT decision-making, that is, preparation for, making and implementing decisions regarding goals, processes, people and technology on a tactical and strategic level. (Simonsson & Johnson, 2006)

"... organisational capacity to control the formation and implementation of IT strategy and provide and achieve competitive advantages for the corporation." (Raghupathi, 2007:96)

"ensuring the establishment of sound organisational structures and processes to support informed decision making about IT investments and the role of IT within an organisation, embedding a comprehensive approach to risk management and performance measurement of IT at an institutional strategic level." (Coen & Kelly, 2007:7)

".... the term used to describe how those entrusted with governance of an entity will consider IT in their supervision, monitoring, control and direction of the entity." (Posthumus, von Solms & King, 2010:23-24)

Summative comment

It is clear from the above that trying to find a standardised definition for IT governance will become a futile exercise of semantics. The definitions of IT governance vary vastly from being an IT strategy which seeks to align business strategy with IT to being structures and processes supporting decision-making regarding various IT-related activities. To seek clarity the definition requires further analysis in order to attain the definition that addresses all core principles defined within the multitude of definitions provided in the literature.

Lee and Lee (2009:47) clarify the ambiguity regarding the definition of IT governance by subdividing the definitions into three perspectives. These perspectives are:

1. The location of decision-making rights and accountabilities within the organisation
   In terms of this perspective, IT governance is defined as the decision-making domain, focusing on the distribution of decision rights and accountabilities (or responsibilities) for the effective use of IT resources
2. The strategic alignment between IT and the business in order to achieve enterprises' full business value
   In this perspective, IT governance is defined as those activities maximising business value through bringing about strategic alignment. To achieve this, emphasis is placed on effective control of resources, performance management and risk management.
3. Those IT organisation structures and processes seeking to achieve the organisations' strategy
   In this perspective IT governance is dealing with the structures of relationships and processes aiming to develop, direct and control IT resources such that IT adds value to the firm's pursuit of its strategic objectives.

In summarising their three perspectives on gaining clarity regarding the view taken on by many authors in defining IT governance, Lee and Lee (2009:48) in short define IT governance as follows:

> *IT governance is the clarification of decision-making rights and responsibilities as companies seek to leverage IT assets to business goals. This alignment is designed to allow organisations to achieve their goals through putting in place a systematic series of activities establishing structures and processes.*

The above definition joins the various perspectives highlighted above into one shared definition to embody IT governance as envisaged in King III, which states that: “IT governance can be considered as a framework that supports the effective and efficient management of IT resources to facilitate the achievement of a company’s strategic objectives” (IoD, 2009:82).

The definition of Lee and Lee will therefore be accepted as the definition of IT governance when referred to in this study.

3.3. THE FOCUS AREAS OF IT GOVERNANCE

Good IT governance forms the foundation of value generation of information technology within an organisation (Bermejo, Tonelli, Brito, Zambalde & Todesco, 2012:11179) and is no longer a “nice to have but a must have” (Almeida, Pereira, & da Silva, 2012:186). Effective IT governance is necessary to “increase value, manage risk, maintain accountability and measure programs and activities” (Croteau, Bergeron & Dubsky, 2013:31). It provides security, reliability and integrity to information and ensures effective management of IT assets (Lainhart, 2000:34). Effective IT governance ensures:

1) the establishment of a trust and transparency relationship among stakeholders of the organisation,
2) the delivery of IT projects within time and budget and
3) desirable behaviour in using IT to align business imperatives and strategies. (Bermejo et al., 2012:11179)

The literature outlines, at a macro level, five focus areas of IT governance (Kordel, 2002; Sandiro-Arndt, 2008; Butler and Butler, 2010:36; Posthumus, von Solms & King, 2010:25-26, Kurti, Barrolli & Sevrani, 2014:2). These areas are:

- **Strategic alignment** *involving making certain that business and IT plans are linked together; defining, maintaining and validating the IT value proposition; and aligning IT operations with overall business operations.*

- **Value delivery** *dealing with executing the value proposition throughout the delivery cycle, making certain that IT delivers its promised benefits against strategy, focusing on optimising costs and verifying the inherent value of IT.*

- **Risk management** *necessitating risk awareness by senior corporate officers, a clear understanding of the organisation's risk appetite, and understanding of compliance requirements, transparency regarding significant organisational risks and embedding of risk management responsibilities into an organisation.*

- **Resource management** *is concerned with the best possible investment in, and the appropriate management of vital IT resources, which would include applications, information, infrastructure and people. Some important points of concern relate to the optimisation of knowledge and the infrastructure.*

- **Performance measurement** *tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using tools such as balanced scorecards that transform strategy into action to achieve goals measurable beyond traditional accounting.*

Summative comment

Due to the lack of clarity in King III regarding how to practically address the implementation of the recommended IT governance principles, an understanding of the focus areas of IT governance assists in highlighting the cornerstones of effective IT governance to the board. Understanding these cornerstones could assist the board in selecting a framework of IT governance which will address all five focus areas.

Having established the cornerstones of focus for effective IT governance, the next step is understanding the mechanism(s) needed to effect IT governance.

3.4. IT GOVERNANCE MECHANISMS

Effective IT governance occurs where a system is in place to determine *who is responsible* for making decisions, *who has input* into those decisions, and *how those people are held accountable* (Weill, 2004:2). This system is critical to the success of an organisation, as it in turn ensures that secure, relevant and reliable information is made available to the right person, at the right time and the right place (Almeida et al. 2013:187). To achieve this system of effective IT governance, the literature argues that a mixture of structure, processes and relational mechanisms must be implemented (Van Grembergen, De Haes & Guldentops, 2004; Webb, Pollard, Ridley, 2006:, Bhattacharya & Chang, 2009:87, Butler & Butler, 2010:35 Almeida et al., 2012:186). These mechanisms are described below:

3.4.1 Governance structures (*who makes the decisions and who is held accountable*)

Governance structures are clearly defined organisational structures, roles and responsibilities created within the organisation to manage the IT investment process (Almeida et al., 2012). It includes structures such as IT committees who oversee various IT functions within the organisation (Bhattacharjya & Chang, 2009:87; Butler & Butler, 2010:35) and roles such as the CIO and IT management staff; however, ultimate responsibility for the board still resides with the board (Posthumus, von Solms & King, 2010:27). The board needs to seek guidance from CIO regarding the effective implementation of these governance structures. King III also refers to other key role players crucial to attaining effective IT governance in the form of the audit, risk, IT steering and strategy committees (IoD, 2009:87, Butler & Butler, 2010:35).

3.4.2 Governance processes (*how decisions are made?*)

Governance processes relates to effective management of the governance structures enabling the timely provision of information as and when needed by the organisation (Webb, Pollard & Ridley, 2006, Butler & Butler, 2010:35). In order to effectively manage these structures, Musson (2009:67-68) stresses five major decisions the board has to make:

- IT principles

- Decides on questions such as the role of IT and the basis of the funding of IT projects.

- IT architecture
  - Discusses the way in which the core business processes are implemented in IT
- IT infrastructure strategies
  - Decides the set of IT infrastructure services needed to support the company's strategic objectives
- Business application needs
  - Determines the set of business applications needed to support the company's business objectives
- IT investment and prioritisation
  - Ensures that the IT investment continues to support the company's changing needs.

The above key decisions have been the subject of numerous research studies, and as it is not within the scope of this research study to explore the detail of each these decisions, a high-level overview is provided in Table 3.1 below as to the decisions the board ought to make to ensure effective IT governance.

Table 3.1: Five major decisions large enterprises have to make with regard to IT governance

Decision	Description of decision	Literature reviewing decision
IT principles	High-level statements about how IT is used in the business	Davenport, Hammer & Metsisto 1989, Broadbent & Weill, 1997
IT architecture	An integrated set of technical choices to guide the organisation in satisfying business needs. The architecture is a set of policies and rules for the use of IT and plots a migration path to	Keen 1995, Ross 2003

	the way business will be done (includes data, technology, and applications)	
IT infrastructure strategies	Strategies for the base foundation of budgeted-for IT capability (both technical and human), shared throughout the firm as reliable services, and centrally coordinated (e.g., network, help desk, shared data)	Keen 1989, Weill, Subramani & Broadbent 2002
Business application needs	Specifying the business need for purchased or internally developed IT applications	Earl 1993
IT investment and prioritisation	Decisions about how much and where to invest in IT including project approvals and justification techniques	Devaraj & Kohli 2002, Ross & Beath 2002

Source: (Weill, 2004)

3.4.3 Governance communication or relational mechanisms *(how the results of governance and IT decisions are monitored, measured and communicated)*

IT governance will be effective only if the related information is measured and communicated throughout the entity (Butler & Butler, 2010:35). Decisions are only as effective as the measures used to monitor and follow up on those decisions (Simonsson & Ekstedt, 2006). The more effective the processes and the communication thereof, the more efficient and effective the IT governance implemented. This, in return, reduces the risk that processes does not work because business and IT do not understand each other and/or are not working together (De Haes & Van Grembergen, 2004). Transparent communication coupled with accountable management of IT governance creates stakeholder confidence and a positive public image (Ragphupathi, 2007:99).

To effectively monitor and follow up on decisions made, the board needs to decide on the type of IT strategy it needs to adopt based on the organisation's need for and reliance on IT to effectively drive the organisational strategic

objectives. Posthumus, von Solms and King (2010:27) suggest that the boards' involvement in IT is defined by two strategies namely, a defensive IT strategy or an offensive IT strategy.

- A ***defensive IT strategy*** focuses on operational reliability, thus ensuring that IT systems continue to function without interruption. It is not necessary to outperform competitors through the intelligent application of emerging technology.
- An ***offensive IT strategy*** focuses more on strategic issues. Offensive IT projects are usually ambitious, involve considerable risk and frequently require significant organisational change. An offensive strategy is necessary when an organisation adjusts its technology strategy for the purpose of enhancing its competitiveness or elevating itself to a position of industry leadership.

Nolan and McFarlan (2005:2-5) also suggest that the board needs to adopt one of the four modes: supportive, factory, turnaround or strategic. The detail regarding the different modes does not form part of the scope of this study and will hence not be discussed in detail.

It must be highlighted that the decision regarding the determination of the correct mixture of mechanisms to achieve effective IT governance can be a complex undertaking, but if effectively implemented and monitored, can result in the alignment of IT and business goals (Almeida et al., 2012:186; Ali & Green, 2012:179).

Summative comment

Effective IT governance is achieved by means of the board realising the correct mixture between structures, processes and relational mechanisms. IT governance mechanisms hone in on who makes what decisions, how those decisions are made and the monitoring of those decisions. The correct mixture might be difficult to attain but when done at the correct level of management, it will attain the required result of effective IT governance.

3.5. IT GOVERNANCE AND THE BOARD

An effective board understands what its role in the organisation is and ensures that it executes the organisations' strategic objectives. As discussed in the previous chapter, King III places the responsibility to ensure effective governance of information technology squarely on the shoulders of the board. Embracing IT oversight as part of its fiduciary duties is indicative of the board's leadership, accountability and responsibility (Posthumus & Von Solms, 2005:17), as this demonstrates their foresight with regard to understanding the enormous impact IT has on strategic decision-making. "Governing technology investment and risk has become part of a board's fiduciary duty of care whether boards realise it or not" (Valentine, 2014:1). A clearer understanding of IT strategy improves the organisation's internal control system, resulting in better support for overall corporate governance objectives (Posthumus & Von Solms, 2005:17). The literature supports this view that the control formulation and implementation of IT strategy, which underpins IT governance, is the responsibility of the board of directors and forms part of corporate governance (De Haes & Van Grembergen, 2004; Parent & Reich, 2009:135; Spremic, 2009:910; Saetang & Haider, 2011:79-80). IT governance is not only a function of conventional corporate governance but forms part of the board's broader governance responsibilities, known as enterprise governance (Lainhart, 2000:33; Weill, 2004; Damianides, 2005:81; Chalaris, Lemos & Chalaris, 2005; Raghuphati, 2007:96; ISACA 2012, Valentine, 2014:1).

3.5.1 Enterprise governance

Broadly defined, enterprise governance is a "set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organisation's resources are used responsibly" (Elgharbawy & Adbel-Kader, 2013:101). Johnston and Hale (2009:126) simply state that enterprise governance is executive management actions that provide strategic direction to the firm, while achieving its objectives, ameliorating risk, and managing resources in the most effective and efficient manner responsible. Further dissecting the term enterprise governance, Sandiro-Arndt (2008:37-38) believes enterprise governance consists of two dimensions i.e.

- *Conformance dimension*, which covers the governance structures and accountability paradigm (corporate governance) and
- *Performance dimension*, covering strategic definition and value creation (business governance).

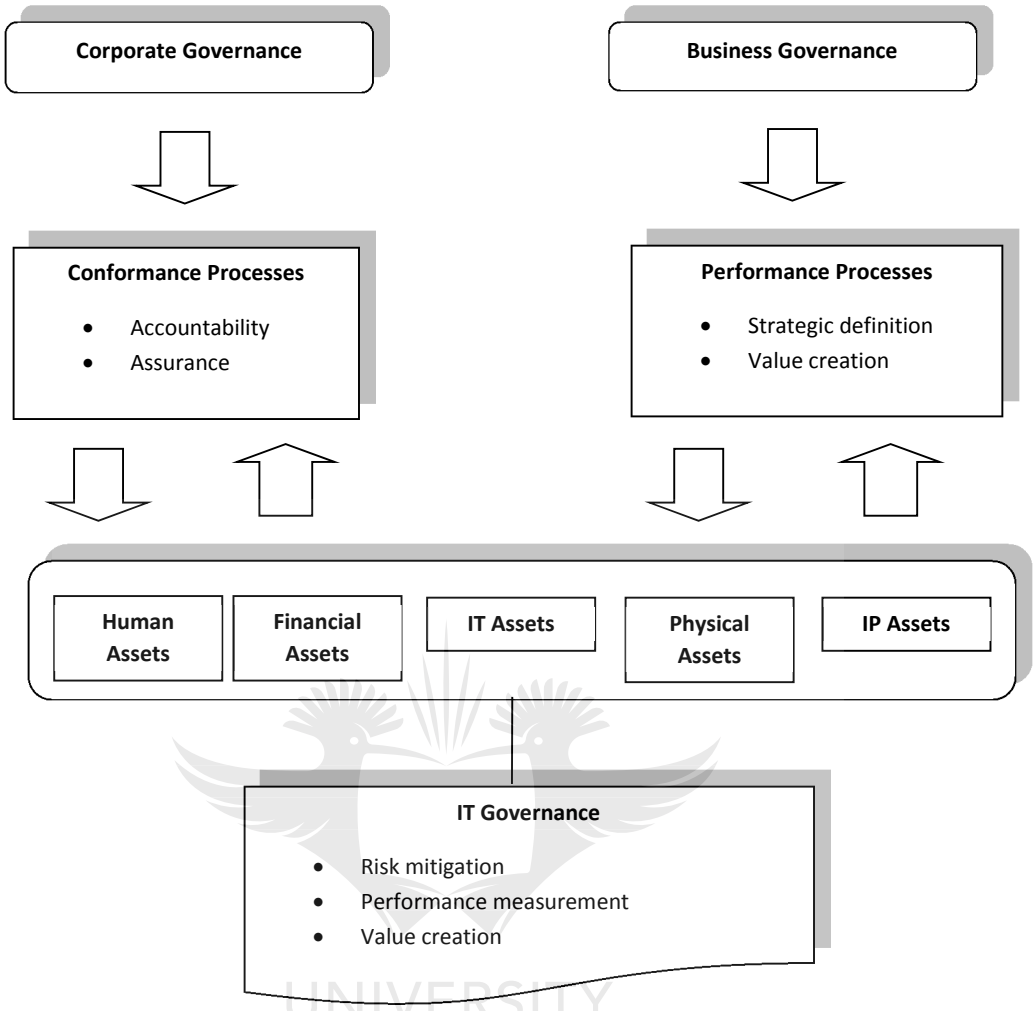
The conformance dimension is concerned with policies, plans and regulation, whereas the performance dimension is concerned with strategy formulation, policy-making and formulating guidelines to direct management decision-making (Elgharbawy & Adbel-Kader, 2013:101). These dimensions should be viewed as complementing one another rather than conflicting with each other.

IT, in return, influences the strategic direction envisaged by the board for the organisation, as the organisation requires IT activities to meet its business objectives (Lainhart, 2000:34). An interdependence can therefore be established, resulting in IT governance forming a sub-set of the overall governance responsibilities of the board. This interdependence is illustrated in Figure 3.1.

Summative comment

IT is a key strategic enterprise asset that must be managed by the board, and as corporate governance is a dimension of enterprise governance (overall governance), it can therefore be established that corporate governance, being the accountability and assurance dimension of enterprise governance, will be the dimension under which IT governance should be managed by the board as part of its overall governance responsibilities. This is in line with King III recommendations.

***Figure 3.1**: Enterprise Governance Framework*



Source: Sandiro-Arndt (2008)

3.5.2 Effectively governing IT as part of corporate governance

Van Grembergen, De Haes and Guldentops (2004:6) highlight that organisations' dependency on IT means that corporate governance issues cannot be solved without considering IT. To make sure that the corporate governance matters are covered, IT needs to be governed properly first. This relationship can be made more accessible by translating the corporate governance questions into specific IT governance questions (Table 3.2).

Table 3.2: IT Governance and Corporate Governance Questions

Corporate Governance questions	⇨	IT Governance questions
How do suppliers of finance get managers to return some of the profits to them?	⇨	How do top management get their CIO and IT organisation to return some business value to them?
How do suppliers of finance make sure that managers do not steal the capital they supply or invest in bad projects?	⇨	How does top management make sure that its CIO and IT organisation do not steal the capital they supply or invest in bad projects
How do suppliers of finance control managers?	⇨	How does top management control its CIO and IT organisation

Source: (Van Grembergen, De Haes & Guldentops, 2004:6)

The questions asked above relate to the establishment of a better control environment, and given that corporate governance is the system through which companies are controlled (Aka, 2007:238), and control is being exercised by senior management within the company aiming to achieve predetermined goals (Rubino & Vitolla, 2014:320), IT governance is implicitly also a dimension of risk management and control and again a responsibility of the board (Satidularn, Wilkin, Tanner, Linger, 2013:421).

3.5.3 The linkage of IT governance key focus areas and IT governance mechanisms with IT governance principles of King III

The principles of King III are grounded in the theory of IT governance discussed in this chapter. Butler and Butler (2010:35-36) deduced that a direct correlation can be drawn between the principles recommended by King III and the IT governance mechanisms (section 3.4) and focus areas (section 3.3). Their findings are summarised in Table 3.3 below:

Table 3.3: Correlation between King III principles, IT governance mechanisms and focus areas

Deductions made	King III principle informing the deduction	IT governance mechanism addressed	IT governance focus area addressed
Where does the responsibility of IT governance lie? *(Whom)*	Principles 5.1, 5.3 and 5.7		
How is IT governance achieved? *(How)*	Principle 5.3	Structure, process & relational mechanisms	
What are the objectives of IT governance *(What?)*	Principles 5.6		Resource management and Strategic alignment
	Principle 5.5		Risk management
	Principle 5.2		Performance management
	Principle 5.4		Value delivery

Source: Butler & Butler (2010:35-36)

Having attained an understanding of the linkage of IT governance theory with the recommended principles of King III in terms of IT governance, one last hurdle remains. King III uses the terms IT governance and IT management interchangeably, although in the literature and COBIT 5 a distinction has been drawn between these disciplines.

3.6. IT GOVERNANCE VERSUS IT MANAGEMENT

It is necessary for a Chinese wall to be built between IT governance and IT management (ITM). King III principle 5.1 states that "The board is responsible for information technology (IT) *governance*", so it's important that the difference between governance and management is clarified. IT governance has already been

defined and hence the focus now shifts to defining ITM. As a point of departure, attention must be drawn to the fact that IT governance and ITM are interrelated disciplines and hence the need to define the terms “management” and “governance” arises. This clarity is necessary to the board as, tasked with the responsibility of effective IT governance, the board should adopt the role of monitoring and focussing on long-term maximisation rather than be hindered with the operational imperatives of management (Waitzer and Enrione, 2005:351).

In drawing a direct comparison between governance and management, Bihari (2008) states that:

> *Governance is concerned with the intrinsic, purpose, integrity and identity of the institution, with a primary focus on the entity’s relevance, continuity, and fiduciary aspects. Governance involves monitoring and overseeing strategic direction, socio-economic and cultural context, externalities, and constituencies of the institution.*
>
> *Management on the other hand, is more of a hands-on activity. In its traditional sense, management can be characterised as conducting or supervising action with the judicious use of means to accomplish certain ends. Management primarily focus on specific goal attainment over a defined time frame and in a prescribed organisation. Planning, staffing, administration and direction, measurement, control, innovation, representation, decision making, and operations are classical elements of management, which essentially strives to function as a closed, command and control system.*

In summary, “governance determines who makes the decisions. Management is the process of making and implementing these decisions” (Dodani, 2006:27). Governance can therefore be viewed as the task of those who provide strategic directions to an organisation, being the board, and management a process/task performed by senior management of an organisation. “While executives and managers administer, develop, implement and monitor business strategies on a day-to-day basis, boards and other governance structures deal with overall organisation policy, culture and direction” (Webb, Pollard & Ridley, 2006).

Coen and Kelly (2007:9-10) further explored these differentiating terms and their views are summarised in Tables 3.4. and 3.5. below:

Table 3.4: The governance perspective

Vision	Alignment	Assurance
Determining the organisation's strategic goals and direction	Seeking alignment of information systems strategy and investment with the organisation's vision and strategy.	Being able to provide assurance to all organisation stakeholders that institutional information systems are aligned to strategy.

Source: Coen and Kelly (2007:9-10)

Table 3.5: The management perspective

Different management perspectives	Areas with which management perspective is concerned		
Resources perspective is concerned with the resources that are required in order to deliver the organisation's information systems.	**People:** ensuring that the expertise and skills of staff are sufficient to effectively use/ or support the information systems and technologies at their disposal.	**Technology:** ensuring that decision about the investment in technology are well – informed and that the technologies the organisation acquires are secure, robust and capable of being used effectively.	**Finance:** ensuring that effective mechanisms are in place to secure, allocate, sustain and manage investment in new and existing systems.
The organisation perspective is concerned with the organisation and procedural structures that are put in place to	**Structures:** ensuring that the organisation's structures effectively support the information systems	**Policies:** ensuring that documented policies and procedures are in place to make each stakeholder aware of their responsibilities and rights in relation to	**Decision – making:** ensuring that suitable individuals or groups are empowered to make decisions and that they are presented with

control the institution's investment in information systems and IT	and services.	the use of information, information systems and IT.	sufficient information and supporting tools to enable them to act effectively.
The service perspective covers all those activities that are 'outputs' of the organisation's investment in information systems and IT	**Systems:** ensuring that organisational systems (both IT-based and manual) offer co-ordinated, supported services to users.	**Projects:** ensuring that procedures are in place to guide, monitor and evaluate information systems 'project' work whether the systems are exploratory pilots or full-scale implementations.	**Service delivery:** ensuring the effective and efficient management of service delivery.

Source: Coen and Kelly (2007:9-10)

ITM is therefore focused on the daily effective and efficient supply of IT services and IT operations involving planning, implementing and measuring policy objectives set by the board, which concentrates on performing and transforming IT to meet present and future demands of the business and the business's customers (Van Grembergen, De Haes & Guldentops, 2004:4).

ITM can therefore be formally defined as:

> *"...being concerned with the exploring and understanding information technology as a corporate resource that determines both the strategic and operational capabilities of the firm in designing and developing products and services for maximum customer satisfaction, corporate productivity, profitability and competitiveness." (Sukhwal & Salvi, 2011:62)*

COBIT 5 differentiates between governance and management by defining the role of each discipline in terms of enterprise governance of IT.

> *"Governance ensures that the stakeholders' needs, conditions and options are evaluated to determine balanced, agreed on enterprise objectives to be*

achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives." (ISACA, 2012)

"Management plans, builds, runs and monitors activities in alignment with the direction set by the governance to achieve the enterprise objectives." (ISACA, 2012)

Summative comment

With reference to the wording provided in King III regarding what defines IT governance, the wording could be considered to contain a certain level of ambiguity because it makes reference to "the effective and efficient *management* of IT resources". The risk therefore arises that a misunderstanding could stem from this principle, forcing the board to get involved in a hands-on capacity and make the decisions regarding IT and the implementation of IT decisions, which is an ITM function. The detailed discussion above helps to clearly define the different roles and focus areas of both ITM as well as IT governance to ensure the noticeable difference in terminology used.

3.7. CRITICAL LINK TO THE STUDY

Establishing a firm grasp of the theory of IT governance, its key focus areas and its mechanisms assists the board to adopt a framework that will ensure a set of comprehensive and interdependent controls are implemented to ensure optimal usage of IT within the organisation. A sound IT governance plan should be based on a solid understanding of the foundations and pillars of IT governance. This chapter provided the basis for that understanding. COBIT 5 positions itself as an enterprise governance framework, and this study will examine to what extent COBIT 5 addresses the requirements of effective governance of IT as recommended by King III in order to suggest to the board a possible "one-stop shop" approach to effective IT governance via the implementation of COBIT 5 as their framework for IT governance.

3.8. CONCLUSION

In this chapter IT governance was conceptualised. This was done by defining IT governance as well as what mechanisms are needed to achieve effective IT governance. It was stressed that no globally accepted definition of IT governance exists, which in terms of King III could pose a problem in terms of measurement. It was however found that though no standardised definition exists, all definitions could be categorised under three main themes; therefore the definition adopted was one which encapsulated all three themes. The five key focus areas of IT governance were explored and why IT governance requires board level attention was established. The link between the theory of IT governance and King III principles was highlighted and a distinction drawn between IT governance and ITM.

King III states that IT governance "can be considered as a framework that supports effective and efficient management" (IoD, 2009:82) and Goosen and Rudman (2013:92) draw attention to the fact that through the implementation of a framework one can ensure adherence to IT governance principles. The framework suggested for adoption is COBIT 5.

CHAPTER FOUR

COBIT: A FRAMEWORK FOR IT GOVERNANCE

4.1. INTRODUCTION

King III highlights that the growth in reliance upon IT has necessitated that the board adopt a more focused approach towards IT governance (IoD, 2009:14-15). To achieve this focused approach the board should attain a thorough understanding around the issues and strategic importance of IT in sustaining the operations of the organisation and by so doing, ensure that its responsibility toward IT governance yields the required returns in terms of IT alignment and IT-related risks being effectively managed (Hardy, 2006:56). Whilst being well aware of how essential IT is to their organisation, boards have been slow to embrace their responsibility towards IT governance, and this has placed them at risk of "flying blind" (Valentine, 2014:3) because they tend to have little interest in IT and even less expertise in terms of this important area of overall governance (Raghuphati, 2007:95). Further exacerbating effective implementation of IT governance is that board members are not provided with specific guidance on how to achieve the vaunted goal of effective IT governance (Hardy, 2006:56). This guidance can be provided in the form of a framework which will assist in the establishment and assessment of control processes, resulting in better implementation of IT governance (Rezaei, 2013:82). In the absence of such a comprehensive and sound IT governance framework, the complexities of modern systems can be overwhelming (Tuttle & Vandervelde, 2007:241).

COBIT constitutes such guidance, as it is an IT governance tool which bridges the gap between control requirements, technical issues, information systems and business risk to facilitate better governance of IT (Lainhart, 2000:22; Hardy, 2006:59; Rubino & Vitolla, 2014:326).

4.2. THE EVOLUTION OF COBIT

COBIT was developed by the Information Systems Audit and Control Association (ISACA), and the international professional membership association for IT professionals and auditors, through the IT Governance Institute (ITGI), as a set of

best practices for information technology management (Sahibudin, Sharifi & Ayat, 2008:749; Rouyet-Ruiz, 2008:41; De Haes & Van Grembergen, 2012:90). COBIT emerged initially from initiatives of ISACA members who were mainly auditors concerned with whether the right control objectives were selected and how those controls were then applied to the computer environment (Kadam, 2012:21). A loose-leaf manual was issued in 1996 to ISACA members of the ISACA then known as "Control Objectives for IS Auditors" (Oliver & Lainhart, 2012:2). COBIT was therefore originally developed as a framework for IS auditors, who were confronted with increasingly automated environments in order to assist them with the execution of IT audit assignments (De Haes, et al., 2013:310) and to serve as a benchmarking tool for IT controls (Tuttle & Vandervelde, 2007:241).

This first version of COBIT was replaced in 1998 with version 2, which was following the trend of version 1, a framework developed by IS auditors for IS auditors, and its key enhancement was the introduction of control practices and control activities relevant to IT controls (Kadam, 2012:21, Oliver & Lainhart, 2012:2). Still firmly rooted in consultancy, COBIT version 2 sustained its strength in two characteristics: control objectives of processes and control criteria of information (Rouyet-Ruiz, 2008:43). As each version evolved to better meet the needs of business through more effective IT governance, one of the biggest key enhancements to COBIT was the positioning of COBIT 3 as a framework for IT governance. COBIT 3 included the notion of IT governance by providing management guidelines, including metrics, critical success factors and maturity models for IT processes (De Haes & Van Grembergen, 2012:90).

COBIT 4 was introduced in 2005, following the trend set by COBIT 3, as an IT governance framework (Kadam, 2012:21), and contained new governance and management concepts such as the alignment of business and IT goals (strategic alignment), value delivery, resource management, risk management, performance management (Rouyet-Ruiz, 2008:41). COBIT 4 also introduced the assignment of roles and responsibilities within IT processes and highlighted the inter-relationship between processes (De Haes & Van Grembergen, 2012:90). COBIT 4 furthermore established four courses of action – namely that IT was:

- focused on business,

- directed towards processes,
- based on controls and
- guided by metrics (Rouyet-Ruiz, 2008:41).

During the period 2005–2010, the ISACA added *Val IT* (which addresses IT-related business processes and responsibilities in value creation) and *Risk IT* (which is focused on risk management) to further enhance the offering of more effective IT governance (De Haes, et al., 2013:310).

Although positioned as the IT governance framework, Oliver and Lainhart (2012:2) emphasise that four main drivers influenced the development of COBIT 5. These were:

- The need for further guidance in areas such as enterprise architecture, asset and service management, emerging sourcing and enterprise models;
- The need for further guidance in terms of innovation and emerging technologies.
- The need to cover the full end-to-end business and IT functional responsibilities as well as the need to cover all aspects leading to effective governance and management of enterprise IT.
- The need to better govern and manage increasing user-initiated and user-controlled IT solutions.

Summative comment

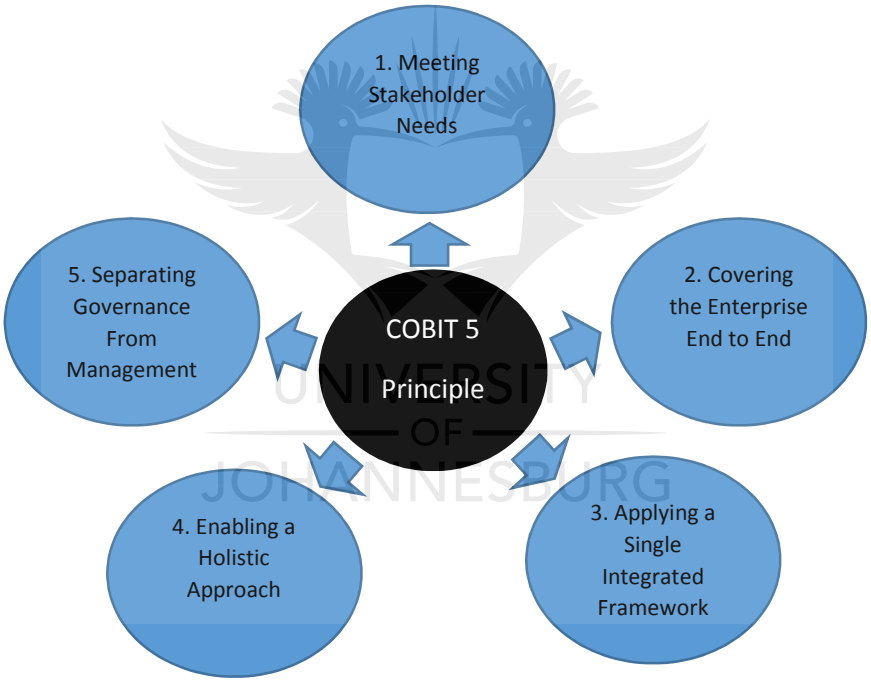
From initially being developed as a set of best-practice control guidelines for IT auditors, COBIT evolved into the de facto framework for IT governance by the release of COBIT 4. COBIT 4, having introduced the five focus areas of IT governance, assigning roles of responsibilities for IT and being complemented by Val IT and Risk IT for better governance of IT governance, was not without its shortcomings. These shortcomings resulted in the development of the latest version of COBIT, COBIT 5, being positioned as the framework for *enterprise governance of IT*.

4.2.1. COBIT 5

In response to the drivers for change, ISACA released the fifth version of COBIT in April 2012, conceptualising it as the enterprise governance of IT. ISACA positions COBIT 5 to be a *"comprehensive framework that assists enterprises to achieve their objectives for the governance and management of enterprise IT. COBIT 5 enables IT to be governed and managed in a holistic manner for the whole enterprise, taking in the full end to end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders"* (ISACA, 2012).

To achieve the objective set out above, COBIT 5 is based on five key principles:

Figure 4.1: COBIT 5 Principles



Source: (ISACA, 2012)

1. **Meeting Stakeholders' Needs**

   All enterprises exist to create value for their stakeholders by means of achieving a balance between the realisation of benefits and the optimisation of risk and use of resources (ISACA, 2012). Creating this value means different things to different stakeholders within an enterprise (Oliver & Lainhart, 2012:5), and this requires the enterprise to analyse its business through defining what the enterprise goals are and linking those

to IT-related goals and IT processes (De Haes, et al., 2013:313). COBIT 5 provides the processes and enablers to support the enterprise in achieving this objective (ISACA, 2012)

2. Covering enterprise end-to-end

The governance of IT is an enterprise-wide function which is clearly articulated in COBIT 5 as it doesn't only focus on the IT function. This function is treated in COBIT 5 like any other asset, and needs to be examined along with the other assets of the enterprise (De Haes, et al., 2013:314). Oliver and Lainhart (2012:6) highlight that to achieve the objective of high-level end-to-end governance an enterprise must address the following fundamentals:

2.1. *Governance enablers*, which relate to the frameworks, policies, principles, structures, processes and practices of organisational resources needing to be present for actions to be directed and objectives to be achieved.

2.2. *Governance scope* in order to outline the different views to which governance should be applied.

2.3. *Governance roles, activities and relationships* explaining the who, what and how of governance.

3. Applying a single framework

COBIT 5 aligns at a high level with relevant standards and frameworks, thus serving as an overarching framework for governance and management of enterprises (Oliver & Lainhart, 2012:7; De Haes, et al., 2013:315-316). COBIT 5 combines the knowledge of frameworks such as Val IT, RiskIT and BMIS and aligns to frameworks such as ITIL, TOGAF and ISO standards in one single integrated framework (ISACA, 2012).

4. Enabling a holistic approach

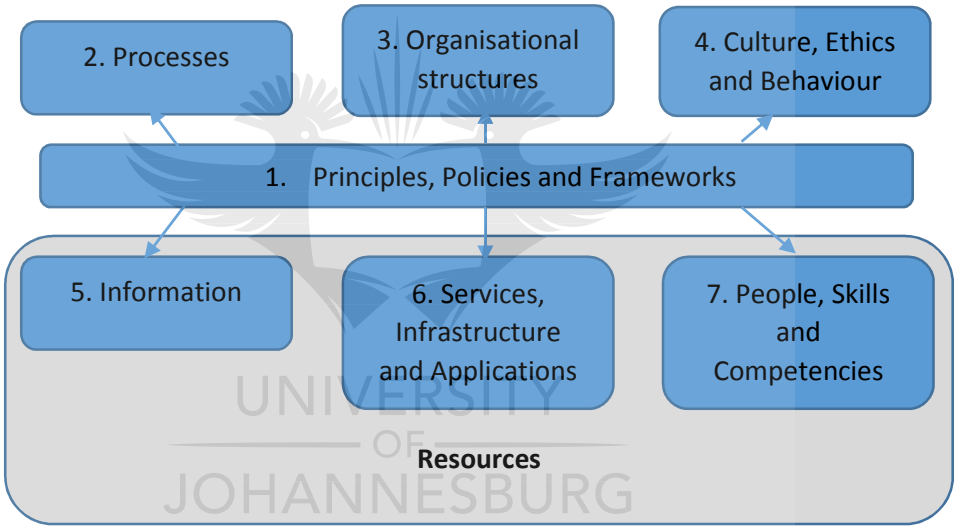
Effective and efficient governance requires a holistic approach, hence the introduction in COBIT 5 of enablers to support the implementation of comprehensive governance of enterprise IT. An enabler is broadly defined in COBIT 5 as a factor that collectively and individually influences

something to work (ISACA, 2012). COBIT 5 identifies seven categories of enablers. These are:

- Principles, policies and frameworks
- Processes
- Organisational structures
- Culture, ethics and behaviour
- Information
- Services, infrastructure and applications, and
- People, skills and competencies.

COBIT 5 illustrates the interplay of these enablers graphically as follows:

Figure 4.2: Seven COBIT 5 Enablers



Source: (ISACA, 2012)

5. **Separating governance from management**

As highlighted in the previous chapter, COBIT 5 draws a distinction between governance and management, as they comprise different types of activities, require different organisational structures and serve different purposes (ISACA, 2012).

4.3. COBIT GOVERNANCE PROCESS

COBIT 5 draws on guidance provided in ISO 38500, the ISO standard for the "Corporate Governance of IT", to organise all governance-related processes under one domain (De Haes, et al., 2013:317). These processes required *Evaluate, Direct*

and Monitor (EDM) practices, which necessitates the involvement of the board of directors in IT governance (De Haes & Van Grembergen, 2012:100; Oliver & Lainhart, 2012:9). COBIT 5 sets about achieving the effective governance by ensuring enterprise objectives such as "evaluating stakeholder needs; setting direction through prioritization and decision making; and monitoring performance, compliance, and progress against plans" are realised (De Haes, et al., 2013:317). These objectives form part of broader stakeholder objectives which according to COBIT 5 should be achieved by way of an effective governance process through which "practices and activities are aimed at evaluating strategic options, providing direction to IT and monitoring the outcome" (ISACA, 2012)

The governance domain consists of five governance processes within which EDM practices are suggested. Each governance practice is supported by guidance with regard to how, why and what is to be implemented in order to improve IT performance (ISACA, 2012). COBIT 5 labels the guidance, "activities", and provides a set of good practice and standard steps deemed necessary to attain governance. Each governance process is linked to related guidance areas such as King III to highlight, for example, the principle(s) of King III being addressed via each process.

Botha (2014:4) highlights that in order for an organisation to implement effective IT governance, an IT governance framework is required that encapsulates structures, processes and mechanism to aid the organisation to meet its overarching objective of creating value for the business. COBIT 5 attempts to be such a framework.

The COBIT 5 processes, together with practices, mapped with King III principles, discussed above, are summarised in Table 4.1 below. The table details the objective of the each process together with the individual EDM sub-objectives requiring board-level attention.

Table 4.1: COBIT 5 governance processes and activities mapped to King III principles

EDM01 Ensure Governance Framework Setting and Maintenance
Analysis and articulation of IT governance requirements within the enterprise to ensure IT-related decisions complement the strategies and objectives of the enterprise. It also highlights oversight activities over IT-related processes to ensure legal, regulatory and board governance requirements are met.

EDM01.01 Evaluate the governance system Establish stakeholder needs, document an understanding of these needs and assess the current and future design of the IT governance within the enterprise.	*EDM01.02 Direct the governance system* Obtain enterprise leaders' buy-in and support and direct governance structures, processes and practices in accordance with agreed-upon decision-making models, design principles and authority levels.	*EDM01.03 Monitor governance system* Monitoring of effectiveness and performance of enterprise IT governance and related mechanisms (structures, processes and principles)
King III related guidance: • 5.1. The board should be responsible for information technology (IT) governance. • 5.3. The board should delegate to management the responsibility for the implementation of an IT governance framework		
EDM02 Ensure benefit delivery Optimisation of return on investment obtained by the organisation from IT services, IT assets and business processes and cost-efficient delivery of services and solutions.		
EDM02.01 Evaluate value optimisation Continual evaluation of IT investments, services and assets in delivering enterprise objectives at a reasonable cost.	*EDM02.02 Direct value optimisation* Channel value management principles and practices towards optimal value creation	*EDM02.03 Monitor value optimisation* Monitoring of key indicators to determine the extent to which expected value and benefits are derived from IT-related investments and services.
King III related guidance: • 5.2. IT should be aligned with the performance and sustainability objectives of the company • 5.4. The board should monitor and evaluate significant investments and expenditure.		
EDM03 Ensure Risk Optimisation Ensures that risk appetite of enterprise is not exceeded, IT risk is identified and managed and compliance failures minimised.		

EDM03.01 Evaluate risk management Evaluation of risk in terms of the use of IT for the enterprise as well as an assessment of the appropriateness of the risk appetite being adopted.	*EDM03.02 Direct risk management* Direct risk management practices to gain assurance that actual IT risk does not exceed enterprise risk appetite	*EDM03.03 Monitor risk management* Monitor key goals and metrics of risk management processes and establish how problems will be identified, tracked and reported
King III related guidance: • 5.5. IT should form an integral part of the company's risk management. • 5.7. A risk committee and audit committee should assist the board in carrying out its IT responsibilities.		
EDM04 Evaluate Resource Optimisation Ensure resource needs (people, processes and technologies) are met in the optimal manner and IT costs are optimised		
EDM04.01 Evaluate resource management Continually establish current and future IT resources, options for resourcing and allocation and management principles to meet needs of enterprise	*EDM04.02 Direct resource management* Ensure the adoption of resource management principles to enable optimal use of IT resources throughout their full economic life cycle.	*EDM04.03 Monitor resources management* Monitor the key goals and metrics of the resource management processes and establish how deviations or problems will be identified, tracked and reported for remediation.
King III related guidance: • 5.6. The board should ensure that information assets are managed effectively.		
EDM05 Ensure Stakeholder Transparency Ensure that enterprise IT performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and the necessary remedial actions.		
EDM05.01 Evaluate stakeholder reporting requirements Continually examine and	*EDM05.02 Direct stakeholders communication and reporting*	*EDM05.03 Monitor stakeholder communication* Monitor the effectiveness

make judgements on the current and future requirements for stakeholder communication and reporting, including both mandatory reporting requirements (e.g. regulatory) and communication to other stakeholders. Establish the principle for communication.	Ensure the establishment of effective stakeholder communication and reporting, including mechanisms for ensuring the quality and completeness of information, oversight of mandatory reporting, and creating a communication strategy for stakeholders.	of stakeholder communication. Assess mechanisms for ensuring accuracy, reliability and effectiveness, and ascertain whether the requirements of different stakeholders are met.
King III-related guidance: • None		

Source: (ISACA, 2012)

4.4. CRITICAL LINK TO THE STUDY

King III recommends as principle 2.1 that the board of directors be the focal point and custodian of corporate governance and with principle 5.1 tasks it (the board) with the responsibility for IT governance. Practical implementation of IT governance principles in terms of King III is a complex exercise, as no clear guidance is provided by the code. The code does however provide 24 recommended practices which, if implemented properly, would attain the principles of effective IT governance. COBIT 5 provides a set of best-practice processes and activities to effectively implement IT governance at a governance level. The recommended practices of King III in terms of attaining the principles set will be matched against the activities of process practices to establish the extent to which the adoption of COBIT 5 governance processes as a basic framework will assist the board to execute its fiduciary duties in terms of the effective governance of IT governance per King III.

4.5. CONCLUSION

The purpose of this chapter was to establish COBIT as a framework for IT governance. In order to achieve this, it was necessary to understand the evolution of COBIT as a governance tool from a best-practice control reference framework to attaining the status as the “de facto standard” for IT governance (Marnewick & Labuschagne, 2011:668).

In its latest edition, COBIT 5 draws a clear distinction between management and governance processes to illustrate at a high level the different organisational structures, activities and purposes required to attain effective IT governance. Given the focus of this study, the governance process practices were summarised together with the related King III guidance links being addressed by each process, according to COBIT 5.

In the following chapter, the recommended practices by King III in terms of IT governance will be mapped to the governance process activities as per COBIT 5 to establish the extent to which the recommended practices as specified by King III are addressed by the governance process practices of COBIT 5 in order to achieve the desired goal of effective IT governance.

CHAPTER FIVE

RESEARCH METHODOLOGY AND RESEARCH FINDINGS

5.1. INTRODUCTION

The objective of this study is to ascertain the extent to which COBIT 5 can be adopted by boards to ensure they execute their duties with regard to the governance of IT as recommended by King III. The literature review performed in chapters 2 – 4 highlight 1) the development of corporate governance with specific focus on the inclusion of IT governance into the King Code, 2) the need for IT governance and involvement the board in terms of taking responsibility for IT governance and 3) the evolution of COBIT as IT governance framework to be adopted as a possible "one-stop shop" for effective IT governance. COBIT 5 has been positioned as an enterprise governance framework able to assist an organisation in unlocking the optimal value from its IT usage whilst maintaining a balance between the benefits realised from IT and minimising the risk associated with the use thereof (ISACA, 2012).

One of the key developments of the new version of COBIT is the fact that it is driven by five basic principles (discussed in chapter 4), one of which is the separation of governance from management. This was deemed necessary because these differing disciplines comprise different types of activities and organisational structures and serve different purposes (ISACA, 2012). Governance, as highlighted by both King III and COBIT 5, is the responsibility of the board. Some of the duties within their fiduciary capacity may be delegated to management, but the board may not absolve itself of these duties. The primary focus of this study is therefore to evaluate the extent to which the activities of the governance process of COBIT 5 address the recommended practices of King III highlighted in chapter 2. In order to achieve this, the following research design and methodology was followed.

5.2. RESEARCH DESIGN AND METHODOLOGY

This research study is a comparative analysis. A literature review was performed focussing on 1) the King Report, its development and the need for the inclusion of chapter five of the Code; 2) the need for IT governance, its key focus areas, mechanisms and the link to the Board; and 3) the development of COBIT as IT

governance framework, in particular highlighting the governance process of COBIT 5 which is the focal point of the mapping against King III recommended practices.

Chapter 2 provided a detailed summary of the IT governance principles of King III together with the recommended practices accompanying these principles. This summary forms the basis of the mapping to COBIT 5's governance process.

The literature review performed on IT governance provided valuable input with regard to understanding the basis of the King III principles for IT governance as it provided the backdrop to the need for IT governance as well as the *what, how and who* to be considered when implementing IT governance. The literature surrounding IT governance was then mapped to the seven principles of IT governance, which established that the King III principles are firmly grounded in the theory.

Although the seven principles are firmly grounded in the theory, the literature review illustrated a lack of clear guidance in terms of the practical implementation of the principles. The 24 best-practice recommendations as provided by King III (chapter 2 of this study) are therefore mapped against 79 governance activities suggested in terms of COBIT 5. This was done to determine the extent to which the best-practice recommendations of King III are addressed by COBIT 5. The mapping done distinguishes the role the board needs to fulfil in terms of COBIT 5 (evaluate, direct or monitor) with regard to each recommended principle of King III.

An assessment was done based on King III-recommended practices not addressed in COBIT 5 to ascertain the completeness of COBIT 5 as an IT governance framework for King III purposes. This exercise was also performed on activities addressed in COBIT 5 for which no recommended practice was suggested by King III to determine whether these activities could possibly strengthen an organisation's governance of IT.

Annexure 1 contains a detailed mapping of COBIT 5 governance process activities to the King III recommended practices detailing what King III requires in terms of principles and recommended practices for IT governance. These were mapped to COBIT 5 activities, which indicates how these principles should be implemented, providing the board with the detailed guidance lacking in terms of King III. The findings of the mapping done are discussed below.

5.3. RESEARCH FINDINGS

The findings from mapping King III recommended activities to COBIT 5 governance activities will be discussed below:

5.3.1. Governance activities addressed by COBIT 5 but not by King III

5.3.1.1. EDM05 Ensure Stakeholder Transparency

As part of governance activities COBIT 5 requires the board to ensure that IT performance and conformance management and the reporting thereof is transparent and measurable by stakeholders against set goals and metrics (ISACA, 2012). COBIT 5 suggests this process to achieve the following objectives in terms of the governance of IT:

- Stakeholder reporting is in line with stakeholder requirements;
- Reporting is complete, timely and accurate; and
- Communication is effective and stakeholders are satisfied.

Focusing purely on the recommended practices of chapter 5 of King III, guidance is provided in King III in terms of ensuring stakeholder transparency. Given the "vagueness" of these recommended principles of King III, it is submitted that these activities could possibly be covered indirectly via recommended practices 5.1.5 and 5.5.2. These inferences are drawn because these practices recommend that external assurance be obtained over IT internal controls and that the organisation should adhere to IT laws, codes and related rules. Adherence to these principles should indirectly be achieved via application of EDM05 activities; however, King III is not clear enough in terms of stakeholder transparency.

More clarity regarding this stakeholder transparency would assist in better governance of IT governance, as COBIT 5 suggests that these activities will aid the board in terms of:

- Evaluating enterprise reporting requirements;
- Enhancing reporting and communication principles;
- Establishing rules for the validation and approval of mandatory reports; and
- Assistance with regard to the assessment of reporting effectiveness (ISACA, 2012).

5.3.1.2. Alignment of resource management with financial and human resources (HR) planning

COBIT 5 addresses governance activities, highlighting the need for board involvement in terms of connecting resource management with HR and financial planning. The sentiment expressed in COBIT is that in the process of IT resource planning/management, it is of the utmost importance that an organisation takes into account its financial and human capital resources.

King III in principle 5.6. addresses management of information assets but fails to link these important elements of effective resource planning to the related recommended practice.

5.3.2. Recommended practices addressed by King III but not by COBIT 5

5.3.2.1. The board should obtain independent assurance on the IT governance and controls supporting outsourced IT services

King III as part of principle 5.1 highlights that the organisation "should understand and manage the risk, benefits and constraints of IT" (IoD, 2009:82). Furthermore, the code requires good governance principles of enforcement and monitoring of effective IT governance even where the provision of IT goods and services has been outsourced (IoD, 2009:85).

COBIT 5 governance activities do not directly address this recommended practice. It is, however, worth mentioning that though not addressed directly, COBIT does state that the board should "monitor IT sourcing strategies, enterprise architecture strategies, IT resources and capabilities to ensure that current and future needs of the enterprise are met" (ISACA, 2012). However, this activity does not address the element of obtaining assurance regarding outsourced services and consequently fails to address the recommended practice adequately.

Summative Comment

The mapping of the King III recommended practices to COBIT 5 governance activities revealed that although King III principles and practices may be vague in terms of not providing the *"how"* to implement the recommended IT governance principles, COBIT 5 can be adopted as an enterprise governance framework. COBIT 5 maps almost perfectly to the recommended practices of King III and can aid the board with practical activities which can be implemented in order to achieve the goal of effective IT governance.

The research findings also indicated that the governance process "Ensure stakeholder transparency" is not addressed by King III. It was found that this process can assist the board with the ability to evaluate reporting requirements and assist with reporting effectiveness. King III also does not recommend practices in terms of aligning human capital and financial resources to resource management, which COBIT 5 does.

King III was found to contain a practice requiring the Board to attain external assurance in relation to IT internal controls, an activity not addressed by COBIT 5's governance processes. It is however evident that although this may be a shortcoming of COBIT 5, adopting COBIT 5 as framework for IT governance will assist the board in meeting its fiduciary duties in terms of King III.

5.4. CONCLUSION

In this chapter the methodology followed to perform the mapping of King III recommended practices to COBIT 5 governance activities was discussed and the research findings analysed.

It was found that although King III principles and practices may be vague in terms of not providing the *"how"* to implement the recommended IT governance principles, COBIT 5 can be adopted as an enterprise governance framework. It was identified that COBIT 5 contains a few more activities not addressed in King III, making it a comprehensive framework for IT governance implementation with reference to the

governance domain. Although a shortcoming was identified in that COBIT 5 does not address the issue of external assurance being obtained for IT controls, COBIT 5 still maps almost perfectly onto the IT governance principles and recommended practices of King III.

In chapter 6 the conclusion to the study will be presented and further areas for research explored.

CHAPTER SIX

CONCLUSION

6.1. INTRODUCTION

This chapter serves to summarise the major literature review findings as well as highlight the results of the research findings presented in chapter 5. It will also make suggestions about future research areas.

6.2. DEDUCTIONS

6.2.1. Literature review

The literature review performed emphasises the reliance of the modern organisation on IT as a strategic partner in its overall business strategy, and that it should be managed at the highest level of management. IT governance enables management to assert the necessary kind of oversight over IT to enable the organisation to attain maximum value from its IT investment at the optimal risk exposure. King III recommends seven principles for the effective governance of IT, supported by 24 best-practice recommendations to achieve the suggested principles. The literature highlighted that though these principles are sound in terms of the theory of effective governance of IT, the recommended practices tend to be ambiguous. IT governance "can be considered as a framework that supports effective and efficient management" (IoD, 2009), and COBIT 5 provides a framework which will assist in the establishment and assessment of control processes, resulting in better implementation of IT governance.

The significant findings of the literature review can therefore be summarised as follows:

- Information systems previously used as enablers to business have now become pervasive in the sense that they are built into the strategy of the business. The pervasiveness of IT in business today mandates the governance of IT as a corporate imperative.
- The board, being tasked by King III with the responsibility of governing risk, ought to be keenly aware of the potential social harms embedded in the organisation's value-creating activities. It should be pro-active in showing

leadership and strategic control in guiding efforts to meet risk management expectations.

- Many executives are intimidated by the task of managing technology because their mind set is that IT requires “special tools, special strategies and a special mind set” (Bensaou & Earl, 1998:120). This creates a basic disconnect between the board and the IT function (Ragphupathi, 2007:95).
- This disconnect can be ascribed to a general lack of adequate strategic skills and insights into IT, resulting in IT risks, with all its intricacies, not being fully understood and effectively mitigated at board level. It must, however, be emphasised that boards recognise the importance and value of IT and in some instances would like to be more actively involved in the oversight thereof but often lack direction in terms of where to begin and how to proceed.
- The King reports are the de facto standard for good governance in South Africa. King III was released in September 2009 and became operational on 1 March 2010 and for the first time provided guidelines regarding the governance of IT in an organisation.
- In as much as the code provides the board with guidelines as to *who* the responsibility of IT governance resides with, as well as *what* should be done, it does not provide adequate guidance on *how* this is to be achieved.
- The Control Objectives for Information and Related Technology (“COBIT”), constitutes such guidance, as it is an IT governance tool which bridges the gap between control requirements, technical issues, information systems and business risk to facilitate better governance of IT.
- COBIT, now in its fifth version, is a comprehensive enterprise governance framework which enables IT to be governed and managed in a holistic manner for the whole enterprise (ISACA, 2012).
- COBIT 5’s governance domain provides five suggested processes which require EDM (Evaluate, Direct and Monitor) practices necessitating the involvement of the board of directors in the governance of IT.
- The five governance processes provide 79 activities that ensure the achievement of the overall domain objective of IT governance at the required level, viz. the board.

6.2.2. Comparative analysis findings

Based on the theoretical foundation provided by the literature review, mapped against the activities of the governance domain of COBIT 5, the following conclusions can be drawn:

- The following governance activities are addressed in COBIT 5 but not in King III:
    - COBIT 5 requires the board to ensure that IT performance and conformance management and the reporting thereof is transparent and measurable by stakeholders against set goals and metrics.
        - As alluded to earlier, recommended practices provided by King III can be vague sometimes and hence there is a possibility that this activity is addressed as part of practices 5.1.5 and 5.5.2 of King III.
        - A more definitive incorporation of these activities into King III can yield the results of:
            - ✓ Evaluating enterprise reporting requirements;
            - ✓ Enhancing reporting and communication principles;
            - ✓ Establishing rules for the validation and approval of mandatory reports; and
            - ✓ Assistance with regard to the assessment of reporting effectiveness.
    - COBIT 5 highlights the need for connecting resource management with HR and financial planning.
        - Principle 5.6 does address management of information assets but fails to link these important elements of effective resource planning to their related recommended practice.
- Recommended practice recommended by King III but not addressed by COBIT 5:
    - King III requires the board to attain an understanding of the IT risks, benefits and constraints and to effectively manage these.
    - It also requires the existence of good governance principles surrounding the outsourcing of IT goods and services.
        - Though not specifically addressed in the level of detail set out in King III, COBIT 5 makes reference to the monitoring of IT

sourcing strategies, resources and enterprise architecture strategies.

- It must however be noted that the governance domain activities do not make reference to the attainment of independent assurance on the IT governance and controls supporting outsourced IT services.

6.3. LINKING RESEARCH PROBLEM TO COMPARATIVE ANALYSIS

The stated research problem sought to identify the extent to which COBIT 5 can be adopted by the board as a framework for IT governance to meet King III requirements. The research findings illustrate that COBIT 5's governance process activities mapped almost perfectly to the King III recommended practices and in some instances even provided more value-add activities than King III. This therefore demonstrates that COBIT 5 can be adopted by the board as a framework for IT governance in terms of King III.

6.4. AREAS FOR FURTHER RESEARCH

The research done in this study is based on the theory of IT governance, King III principles and COBIT 5 governance domain activities. The research study seeks to establish the adoption of COBIT 5 as a framework for effective IT governance in terms of King III. As a result, opportunities exists for further research with regard to the feasibility of adopting COBIT 5 practically as a governance framework for IT as well as the extent to which the King IV committee incorporates the value-add activities of COBIT 5 into IT governance principles.

6.5. CONCLUSION

This study endeavoured to discover the extent to which COBIT 5, with specific focus on its governance domain, can be adopted by the board as a framework for effective governance of IT in terms of King III. The study revealed that COBIT 5 as a framework does indeed address the recommended principles and practices of King III and in some instances provides more focused guidance on reporting requirements that warrant inclusion into King III. The framework, at its core, does indeed assist the board in understanding the *how* of IT governance that, as indicated by the literature, King III does not provide sufficient guidance on.

REFERENCE LIST

Afzali, P., Azmayandeh, E., Nassiri, R., & Shabgahi, G. L. (2010, November). *Effective governance through simultaneous use of COBIT and Val IT. International Conference on Education and Management Technology*: 46-50

Aguilera, RV., Filatotchev, I., Gospel, H., & Jackson, G. (2008). An organizational approach to comparative corporate governance: Costs, contingencies, and complementarities. *Organization Science*, 19(3): 475 – 492.

Aka, PC. (2007). Corporate Governance in South Africa: Analyzing the Dynamics of Corporate Governance Reforms in the "Rainbow Nation". *North Carolina Journal of International Law and Commercial Regulation,* 33: 220 – 292.

Al Omari, L., Barnes, PH., & Pitman, G. (2012). An exploratory study into audit challenges in IT governance: a Delphi approach. Available from: http://eprints.qut.edu.au/53110/1/An_Exploratory_Study_into_Audit_Challenges_in_IT_Governance_A_Delphi_Approach.pdf

Ali, S., & Green, P. (2012). Effective information technology (IT) governance mechanisms: An IT outsourcing perspective. *Information Systems Frontiers*,14(2), 179 – 193.

Almeida, R., Pereira, R., & da Silva, MM. (2013). IT Governance Mechanisms: A Literature Review. In Exploring Services Science: 186 – 199. Springer Berlin Heidelberg.

Al Omari, L., Barnes, PH., & Pitman, G. (2012, December). *Optimising COBIT 5 for IT governance: examples from the public sector. In Proceedings of the ATISR 2012: 2nd International Conference on Applied and Theoretical Information Systems Research (2nd. ATISR2012).* Academy of Taiwan Information Systems Research.

Alpaslan, CM., Green, SE., & Mitroff, II. (2009). Corporate governance in the context of crises: towards a stakeholder theory of crisis management. *Journal of Contingencies and Crisis Management,* 17(1): 38 – 49.

Andreasson, S. (2011). Understanding Corporate Governance Reform in South Africa Anglo-American Divergence, the King Reports, and Hybridization. *Business & Society,* 50(4):647 – 673.

Andriole, SJ. (2009). Boards of directors and technology governance: The surprising state of the practice. *Communications of the Association for Information Systems,* 24(1): 373 – 394.

Bajo, E., Bigelli, M., Hillier, D., & Petracci, B. (2008). The Determinants and Value Impact of Regulatory Compliance: An Analysis of Insider Trading Disclosures: 1 – 41.

Bensaou, BM., & Earl, M. (1998). Information Technology in Japan: Are there Lessons for the West?. *In Information Technology and Industrial Competitiveness*. 153 – 174. Springer US.

Bermejo, PHDS., Tonelli, AO., Brito, MJD., Zambalde, AL., & Todesco, JL. (2012). Implementation of information technology (IT) governance through IT strategic planning. *African Journal of Business Management,* 6(45): 11179 – 11189.

Bhattacharjya, J., & Chang, V. (2009). *Adoption and Implementation of IT Governance: Cases from Australian Higher Education. In Information Technology Governance and Service Management: Frameworks and Adaptations: 82-100.* Edited by A. Cater-Steel. Hershey, PA: Information Science Reference. doi:10.4018/978-1-60566-008-0.ch003

Bharadwaj, A., El Sawy, OA., Pavlou, PA., & Venkatraman, N. (2013). Digital business strategy: toward a next generation of insights. *MIS Quarterly,* 37(2): 471 – 482.

Bihari, E. (2008). Information security governance and Boards of directors: Are they compatible? Available from: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1045&context=ism

Botha, DP. (2014). *Bridging the Information Technology (IT) gap in South Africa through a step by step approach to IT governance.* (Master's dissertation).

Stellenbosch: Stellenbosch University. Available from: http://scholar.sun.ac.za/handle/10019.1/86464

Brennan, Niamh M., & Solomon, J. (2008). Corporate governance, accountability and mechanisms of accountability: an overview. *Accounting, Auditing & Accountability Journal,* 21.7: 885 – 906.

Butler, R. & Butler, MJ. (2010). Beyond King III: Assigning accountability for IT governance in South African enterprises. *South African Journal of Business,* 41(3): 33 – 45.

Chauke, A. (10 February 2012). Inside the R42m heist. *Timeslive*. Available from: http://www.timeslive.co.za/local/2012/02/10/exclusive-inside-the-r42m-heist

Chalaris, I., Lemos, PP., & Chalaris, M. (2005). IT Governance: The Safe Way to Effective and Efficient Governance. *E-Journal of Science and Technology,* 1(1), 59 - 63.

Chitambala, G. (2006). *Status of IT governance in South Africa : a comparative view*. (MBA dissertation). Pretoria: University of Pretoria. Available from:

http://upetd.up.ac.za/thesis/available/etd-04012010-145141/unrestricted/dissertation.pdf

Coen, M. & Kelly, U. (2007). Information management and governance in UK higher eductation institutions: bringing IT in from the cold. *Perspectives,* 11(1): 7 – 11.

Coertze, J., & von Solms, R. (2013). The Board and IT Governance: A Replicative Study. *African Journal of Business Management,* 7(35): 3358-3373.

Coertze, J., & Solms, RV. (2014). *The Board and CIO: The IT Alignment Challenge. 47th Hawaii International Conference on System Sciences:* 4426-4435. IEEE.

Corina, G. & Roxanna, S. 2011. Comparative study on corporate governance. *Economic Science Series*, 20(2): 674 – 680.

Croteau, AM., Bergeron, F., & Dubsky, J. (2013). Contractual and Consensual Profiles for an Interorganizational Governance of Information Technology. *International Business Research,* 6(9): 30 – 43.

Damianides, M. 2005. Sarbanes-Oxley and IT governance: New guidelines on IT control and compliance, *Information Systems Management,* 22(1): 77-85.

De Haes, S., & Van Grembergen, W. (2004). IT governance and its mechanisms. Available from: http://pdf.aminer.org/000/245/098/introduction_to_the_minitrack_it_governance_and_its_mechanisms.pdf

De Haes, S. & Van Grembergen, W. (2008). Practices in IT Governance and Business /IT Alignment. *Information Systems Control Journal,* Volume 2

De Haes, S., & Van Grembergen, W. (2012). An Academic Exploration into the Core Principles and Building Blocks of COBIT 5. *International Journal of IT/Business Alignment and Governance,* 3(2): 51-63.

De Haes, S., Van Grembergen, W., & Debreceny, RS. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems,* 27(1):307 – 324.

Denis, D. & McConnell, JJ. (2002). International Corporate Governance. *Journal of Financial and Quantitative Analysis,* 38(1):1 – 36.

Dhillon, G. & Backhouse, J. (1996). Risks in the use of information technology within organizations. *International Journal of Information Management,* 16(1): 65 – 74.

Diamond, G., & Price, G. (2012). The political economy of corporate governance reform in South Africa. *South African Journal of Business Management,* 43(1): 57 – 67.

Dodani, MH. (2006). Who Took the Cookie from the Cookie Jar?. *Journal of Object Technology,* 5(4): 23 – 28.

Elgharbawy, A., & Abdel-Kader, M. (2013). Enterprise governance and value-based management: a theoretical contingency framework. *Journal of Management & Governance,* 17(1): 99 – 129.

Gavrea, C., & Stegerean, R. (2011). The relationship between corporate governance and organizational performance: evidence from literature. *Managerial Challenges of the Contemporary Society,* (2): 92 – 99.

Goeken, M. & Alter, S. (2008). *IT governance framework as methods, Proceedings of the International Conference on Enterprise Information Systems* held in, Barcelona, Spain: 331 - 338

Gomes, J.R. (2007). *The state of IT governance in South Africa.* (MBA dissertation) Pretoria: University of Pretoria. Available from:

http://upetd.up.ac.za/thesis/available/etd-03232010-/130049/unrestricted/dissertation.pdf

Goosen, R., & Rudman, R. (2013). The development of an integrated framework in order to address King III's IT governance principles at a strategic level. *South African Journal of Business Management,* 44(4): 91 – 103.

Gregory, HJ. & Simms, ME. (1999). *Corporate Governance: What it is and why it matters. 9th International Anti-Corruption Conference* held in Kuala Lumpur

Gstruanthaler, T. (2010). Corporate Governance in South Africa: The introduction of King III and reporting practices at the JSE Alt-X. *Corporate Ownership & Control,* 7(3): 146 – 153.

Hardy, G. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security technical report,* 11(1): 55 – 61.

Huff, SL., Maher, PM., & Munro, MC. (2004). What boards don't do – but must do – about Information Technology. *Ivey Business Journal,* 69(1): 1-4.

Institute of International Finance (IIF). September 2007. Corporate Governance in South Africa – An Investor Perspective

Institute of Directors. (IoD). (2009). *King III Report on Corporate Governance*, Institute of Directors in Southern Africa. Johannesburg

IT Spending and Staffing Benchmark 2013/2014 Available at: http://www.computereconomics.com/page.cfm?name=issexecsumy

ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.* Rolling Meadows, IL: ISACA

Jianmu, Y. (2007). *A Research on Enterprise IT Governance and Its Framework. In proceedings of International Conference on Wireless Communications, Networking and Mobile Computing,* 4284 - 4287.

Johnston, AC., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM,* 52(1): 126 – 129.

Kadam, AW. (2012, September). The Evaluation of COBIT. *CSI Communications:* 21 – 22.

Kadam, A. (2012, October). Why Do We Need the COBIT 5 Business Framework. *CSI Communications:* 25-27.

Kakabadse, A. & Korac-Kakabadse, N. (2002). Corporate governance in South Africa: Evaluation of King II Report. *Journal of Change Management,* 2(4):305 – 316.

Kaselowski, E., Von Solms, B., & Von Solms, R. (2010). Municipalities and information technology governance-towards a strategic planning framework. *Journal of Public Administration,* 45(2): 334 – 342.

Khanyile, S., & Abdullah, H. (n.d.). COBIT 5: an evolutionary framework and only framework to address the governance and management of enterprise IT. Available from: http://osprey.unisa.ac.za/TechnicalReports/Cobit5.pdf

Khumalo, V.M. (2012). *The capability levels of IT governance for South African organisations.* (MBA dissertation). Pretoria: University of Pretoria. Available from: http://upetd.up.ac.za/thesis/available/etd-02232013-115244

Kordel, L. (2002). IT Governance Hands-on: Using Cobit to Implement IT Governance. *Information Systems Control Journal,* Vol 2.

Kurti, I., Barrolli, E., & Sevrani, K. (2014). Effective IT Governance in the Albanian Public Sector – A Critical Success Factors Approach. *The Electronic Journal of Information Systems in Developing Countries,* 63(6): 1-22.

Kyereboah-Coleman, A. (2007). *Relationship between corporate governance and firm performance: an African perspective* (Doctoral dissertation). Stellenbosch: Stellenbosch University.

Available from: https://scholar.sun.ac.za/handle/10019.1/1348

Lainhart, IV. (2000). COBIT™: A methodology for managing and controlling information and information technology risks and vulnerabilities. *Journal of Information Systems,* 14(1): 21-25.

Lainhart, IV., & John, W. (2000). Why IT governance is a top management issue. *Journal of Corporate Accounting & Finance,* 11(5): 33-40.

Lee, TB. (17 December 2014). The Sony hack: how it happened, who is responsible and what we've learnt. *Vox.* Available from: http://www.vox.com/2014/12/14/7387945/sony-hack-explained

Lee, J., & Lee, C. (2009). *IT Governance-Based IT Strategy and Management: Literature Review and Future Research Directions. In Information Technology Governance and Service Management: Frameworks and Adaptations*: 44-62. Edited by A. Cater-Steel. Hershey, PA: Information Science Reference. doi:10.4018/978-1-60566-008-0.ch002

Mahadeo, JD., Soobaroyen, T., & Hanuman, VO. (2012). Board composition and financial performance: Uncovering the effects of diversity in an emerging economy. *Journal of business ethics,* 105(3): 375-388.

Marnewick, C., & Labuschagne, L. (2011). An investigation into the governance of information technology projects in South Africa. *International Journal of Project Management,* 29(6):661-670.

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

Park, Johannesburg: University of Johannesburg. Available from: http://hdl.handle.net/10210/3184

McDonnell, U. (2006, March). Sound IT Governance Requires Breadth Depth. *Financial Executive*: 54-56

Miles, L. & Jones M. (2009). Prospects for Corporate Governance Operating as a Vehicle for Social Change in South Africa, *Deakin Law Review,* 14(1):53-77.

Mostovicz, EI., Kakabadse, NK., & Kakabadse, AP. (2010). The four pillars of corporate responsibility: ethics, leadership, responsibility and trust. *The international journal of business in society,* 11(4): 489 – 500.

Motloutsi, VM. (2009). *The state of IT governance in the top 20 IT spending companies in South Africa.* (MBA dissertation). Pretoria: University of Pretoria. Available from: http://upetd.up.ac.za/thesis/available/etd-05062010-142632

Musson, D. (2009). IT Governance: A Critical Review of the Literature. In Information Technology Governance and Service Management: Frameworks and Adaptations: 63-81. Edited by Cater-Steel (Ed.). Hershey, PA: Information Science Reference. doi:10.4018/978-1-60566-008-0.ch003

Nel, I. (2011). *An investigation into the business continuity risks and related business continuity plan* (Masters Dissertation). Auckland Park, Johannesburg: University of Johannesburg. Available from: http://hdl.handle.net/10210/5067

Nolan, F. & McFarlan, FW. (2005). Information Technology and the Board of Directors. *Harvard Business Review.* Available from: http://www3.fsa.br/LocalUser/gestaoti/Ativ03%20NOLAN%202005%20%20Information%20Technology%20and%20the%20Board%20of%20Directors..pdf

Nikolić, J., & Erić, J. (2011). Boards of directors models and role in corporate governance. *Management-časopis za teoriju i praksu menadžmenta,* 16(60):69-75.

Ntim, CG., Opong, KK., Danbolt, J., & Thomas, DA. (2012). Voluntary corporate governance disclosures by post-apartheid South African corporations. *Journal of Applied Accounting Research,* 13(2): 122-144.

Oliver, D., & Lainhart, J. (2012). COBIT 5: Adding value through effective Geit. *EDPACS,* 46(3): 1-12.

Parent, M., & Reich, B. H. (2009). Governing Information Technology Risk. *California Management Review,* 51(3):134-152.

Planting, S. (18 January 2012). How R42m was stolen from Postbank. Available from: http://www.moneyweb.co.za/mw/content/en/moneyweb-special-investigations?oid=560023&sn=2009+Detail

Posthumus, S. & Von Solms, R. (2005). IT oversight: an important function of corporate governance. *Computer Fraud & Security,* 2005(6): 11-17.

Posthumus, S., von Solms, R. & King, M. (2010). The board and IT governance: The what, who and how. *South African Journal of Management,* 41(3):23-32.

Raghupathi, W. (2007). Corporate Governance of IT: A Framework for Development. *Communications of the ACM,* 50(8):94 – 99.

Reznik, S. (2007). Back to business with IT governance. *Journal of Corporate Accounting & Finance,* 18(5): 57-64.

Rezaei, N. (2013). The Evaluation of Implementing IT Governance Controls. *Journal of Applied Business and Finance Researches*, *2*(3): 82-89.

Rouyet-Ruiz, J. (2008). COBIT as a Tool for IT Governance: between Auditing and IT Governance. *The European Journal for the Informatics Professional,* 9(1): 40-43.

Rossouw, GJ., van der Watt, A. & Malan, DP.(2002). Corporate Governance in South Africa. *Journal of Business Ethics,* 37:289-302.

Rossouw, D. (2009). Internal corporate governance and personal trust. *African Journal of Business Ethics,* 4(1): 37–45.

Rubino, M., & Vitolla, F. (2014). Corporate governance and the information system. How a framework for IT governance supports ERM. *Corporate Governance,* 14(3): 320-338.

Rushton, K. (21 October 2014). Apple iCloud 'hacked' in China. *The Telegraph.* Available from: http://www.telegraph.co.uk/technology/apple/11178451/Apple-iCloud-hacked-in-China.html

Saetang, S., & Haider, A. (2011). *Conceptual aspects of IT governance in enterprise environment. Proceedings of the 49th SIGMIS annual conference on Computer personnel research*: 79-82.

Sahibudin, S., Sharifi, M., & Ayat, M. (2008). *Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. Second Asia International Conference on Modelling and Simulation:* 749-753.

Samuwai, J., Prasad, A., Green, P., & Heales, J. (2012). *Towards an Effective Structure of IT Governance for Organizations in Developing Economies. AMCIS 2012 Proceedings.* Paper 7 Available from: http://aisel.aisnet.org/amcis2012/proceedings/ICTinGlobalDev/7

Sandiro-Arndt, B. (2008). People, Portfolios and Processes: The 3P Model of IT Governance. *Information Systems Control Journal,* 2:36-39.

Satidularn, C., Wilkin, C., Tanner, K., & Linger, H. (2013). Investigation of the Relationship between IT Governance and Corporate Governance. *Management, Leadership and Governance,* 420–423.

Schooley, D., Renner, C. & Allen, M. (2010). Shareholder Proposals, Board Composition, and Leadership Structure. *Journal of Managerial Issues,* 2: 152-165.

Shapatoti, H. (2011). Corporate Governance: What it is and why it matters. *International Journal of Governance,* 1(3): 527-537.

Simonsson, M., & Johnson, P. (2006, June). *Defining IT governance-a consolidation of literature. In the 18th Conference on Advanced Information Systems Engineering.* Available from:

http://www.ics.kth.se/Publikationer/Working%20Papers/EARP-WP-2005-MS-04.pdf

Simonsson, M. & Ekstedt, M. (2006). *Getting the Priorities Right: Literature vs Practice on IT Governance. Proceedings of the Technology Management for the Global Future (PICMET),* Portland, USA.

Spremic, M. (2009). IT Governance Mechanisms in Managing IT Business Value. *Information Science and Applications,* 6(6):906-915.

Steenkamp, G. (2009). *Mapping the Information Technology (IT) governance requirements contained in the King III Report to the IT domains and processes of the Control Objectives for Information and Related Technology (COBIT) framework* (Masters Dissertation). Stellenbosch: University of Stellenbosch. Available from: https://scholar.sun.ac.za/handle/10019.1/15050

Sukhwal, BK. & Salvi, L. (2011). Information Technology Management. *International Journal of Computer Applications and Natural Sciences,* 1(1):62 - 65

Swart, W. & Wa Afrika, M. (2012, January 15). It was a happy New Year's Day for gang who pulled off...R42m Postbank heist. *Timeslive.* Available from: http://www.timeslive.co.za/local/2012/01/15/it-was-a-happy-new-year-s-day-for-gang-who-pulled-off...r42m-postbank-heist

Symons, C. (2005). IT Governance Framework; Structure, Processes, and Communication. Cambridge USA: Forrester Research Inc.
Available at: http://infochief.com.vn/News/IT%20Governance%20Framework.pdf

Tuttle, B., & Vandervelde, SD. (2007). An empirical examination of CobiT as an internal control framework for information technology. *International Journal of Accounting Information Systems,* 8(4): 240-263.

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

Valentine, E. (2014). Are Boards Flying Blind When it Comes to Enterprise Technology Governance? *EDPACS,* 49(2):1-5.

Van Grembergen W, De Haes S, Guldentops E. (2004). Structures, processes and relational mechanisms for IT governance. *Strategies for Information Technology Governance.* Hershey, PA: Idea Group Publishing: 1-36.

Van Reenen, R. (2007). eNaTIS – Would prevention have been the cure? *Enterprise Risk*, 1(3): 38-39.

Vaughn, M. and Ryan, LV. (2006), Corporate Governance in South Africa: a bellwether for the continent? *Corporate Governance: An International Review,* 14(5): 504–512. doi: 10.1111/j.1467-8683.2006.00533.x

Waitzer, E. J., & Enrione, A. (2005). Paradigm flaw in the boardroom: Governance versus management. *International Journal of Disclosure and Governance,* 2(4): 348-356.

Webb, P., Pollard, C. & Ridley, G. (2006). Attempting to Define IT Governance: Wisdom or Folly?. Available from: http://18.7.29.232/bitstream/handle/1721.1/1846/4237-02.pdf?sequence=2

Weitzner, D. & Peridis, T. (2011). Corporate Governance as Part of the Strategic Process: Rethinking the Role of the Board. *Journal of Business Ethics,* 102:33-42.

Weill, P., & Woodham, R. (2003). Don't just lead, govern: Implementing effective IT governance. Available from: http://18.7.29.232/bitstream/handle/1721.1/1846/4237-02.pdf?sequence=2

Weill, P. (2004). Don't just lead, govern: How top-performing firms govern IT. *MIS Quarterly Executive,* 3(1): 1-17.

West, A. (2006). Theorising South Africa's Corporate Governance. *Journal of Business Ethics,* 68:433-448.

West, A. (2009). The ethics of corporate governance: A (South) African perspective. *International Journal of Law and Management,* 51(1): 10-16.

Yasser, Q. R. (2011). Corporate governance and performance (a case study for Pakistani communication sector). *International Journal of Trade, Economics and Finance,* 2(3): 204-211.

ANNEXURE 1: MAPPING OF KING III RECOMMENDED PRACTICES TO COBIT 5 GOVERNANCE ACTIVITIES

IT Governance Principle	Recommended Practice (RP) (What should be done)	COBIT 5 Practice	COBIT 5 Governance Activity EVALUATE	COBIT 5 Governance Activity DIRECT	COBIT 5 Governance Activity MONITOR
WHAT SHOULD BE DONE?		**HOW IT SHOULD BE DONE**			
5.1. The board should be responsible for IT governance	5.1.1. The board should assume responsibility for the governance of IT and place it on the board agenda	EDM01.01 EDM01.02 EDM01.03	Analyse and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence governance design. Determine the significance of IT and its role with respect to the business. Consider external regulations, laws and contractual obligations and determine how they should be applied within the governance of enterprise IT. Articulate principles that will guide the design of governance and	Communicate governance of IT principles and agree with executive management on the way to establish informed and committed leadership	Assess the effectiveness of the governance design and identify actions to rectify deviations.

			decision making.		
	5.1.2. The board should ensure that an IT charter and policies are established and implemented	EDM01.01 EDM01.02 EDM01.03	Understand the enterprise's decision-making culture and determine the optimal decision-making model for IT.	Direct that staff follow relevant guidelines for ethical and professional behaviour and ensure that consequences of non-compliance are known and enforced.	Maintain oversight of the extent to which IT satisfies obligations (regulatory, legislation, common law, contractual), internal policies, standards and professional guidelines. Monitor regular and routine mechanisms for ensuring that the use of IT complies with relevant obligations (regulatory, legislation, common law, contractual), standards and guidelines.
	5.1.3. The board should ensure promotion of an ethical culture and awareness a common IT language	EDM01.01 EDM01.02 EDM01.03	Align the ethical use and processing of information and its impact on society, natural environment, internal and external stakeholder interest with the enterprise's direction, goals and objectives.	Direct the establishment of a reward to promote desirable cultural change	Maintain oversight of the extent to which IT satisfies obligations (regulatory, legislation, common law, contractual), internal policies, standards and professional guidelines.
	5.1.4. The board should ensure than an IT internal control framework is	EDM01.01 EDM01.02 EDM01.03	Determine the implications of the overall enterprise control with regard	Establish or delegate the establishment of governance	Periodically assess whether agreed-on governance of IT mechanisms

	adopted and implemented		to IT.	structures, processes in line with agreed upon design principles	(structures, principles, processes, etc) are established and operating effectively.
	5.1.5. The board should receive assurance on the effectiveness of the IT internal controls.	EDM01.03			Provide oversight of the effectiveness of, and compliance with, the enterprise's system of control. Assess the effectiveness and performance of those stakeholders given delegated responsibility and authority for governance of enterprise IT.
5.2. IT should be aligned with the performance and sustainability objectives of the company	5.2.1 The board should ensure that the IT strategy is integrated with the company's strategic objectives and business processes.	EDM02.01 EDM02.03	Evaluate how effectively the enterprise and IT strategies have been integrated and aligned with enterprise goals for delivering value. Consider how well the management of IT-enabled investments, services and assets align with the enterprise value management and financial management		Obtain regular and relevant portfolio, programme and IT (technological and functional) performance reports. Review the enterprise's progress towards identified goals and the extent to which planned objectives have been achieved, deliverables obtained, performance targets met and risk

			practices.		mitigated.
	5.2.2. The board should ensure that there is a process to identify and exploit opportunities to improve the performance and sustainability of the company through the use of IT.	EDM02.01 EDM02.02	Understand and regularly discuss the opportunities that could arise from enterprise change enabled by current, new or emerging technologies, and optimise the value created from those opportunities	Direct management to consider potential innovative uses of IT that enable the enterprise to respond to new opportunities or challenges, undertake new business, increase competitiveness or improve processes. Recommend consideration of potential innovations, organisational changes or operational improvements that could drive value for the enterprise from IT-enabled initiatives.	
5.3. The board should delegate to management the responsibility for the implementation of an IT governance framework	5.3.1. Management should be responsible for the implementation of the structures, processes and mechanisms for the IT governance framework.	EDM01.02 EDM01.03		Establish or delegate the establishment of governance structures, processes in line with agreed upon design principles	Periodically assess whether agreed-on governance of IT mechanisms (structures, principles. processes, etc) are established and operating effectively.
	5.3.2. The board may appoint an IT steering committee of similar function to	EDM01.01 EDM01.02 EDM01.03	Determine the appropriate levels of authority delegation, including threshold	Communicate governance of IT principles and agree with executive	Assess the effectiveness of the governance design and identify actions

	assist with its IT governance		rules, for IT decisions	management on the way to establish informed and committed leadership	to rectify deviations.
	5.3.3. The CEO should appoint a CIO responsible for the management of IT.				
	5.3.4. The CIO should be suitably qualified and experienced person who should have access and interact regularly on strategic IT matters with the board and/or appropriate board committee and executive management.	EDM01.02		Ensure that communication and reporting mechanisms provide those responsible for oversight and decision making with appropriate information.	
5.4. The board should monitor and evaluate significant IT investments and expenditure	5.4.1. The board should oversee the value delivery of IT and monitor the return on investment from significant IT projects.	EDM02.01 EDM02.02 EDM02.03	Understand what constitutes value for the enterprise, and consider how well it is communicated, understood and applied throughout the enterprise's processes. Evaluate the portfolio of investments, services and assets for alignment with the enterprise's objectives; enterprise worth, both financial and non-financial; risk,	Define and communicate portfolio and investment types, categories, criteria and relative weightings to the criteria to allow for overall relative value scores. Define requirements for stage-gates and other reviews for significance of the investment to the enterprise and associated risk, programme schedules, funding	ALL EDM 02.03 activities

			both delivery and benefits risks; business process alignment; effectiveness in terms of usability, availability and responsiveness; and efficiency in terms of cost, redundancy and technical health	plans and the delivery of key capabilities and benefits and ongoing contribution to value. Define and communicate enterprise-level value delivery goals and outcome measures to enable effective monitoring. Direct any required changes to the portfolio of investments and services to realign with current and expected enterprise objectives and/or constraints.	
	5.4.2. The board should ensure that intellectual property contained in information systems is protected.	EDM02.01 EDM04.02	Understand the key elements of governance required for the reliable, secure and cost effective delivery of optimal value from the use of existing and new IT services, assets and resources.	Establish principles related to safeguarding resources	
	5.4.3. The board should obtain independent assurance on the IT governance and controls supporting				

	outsourced IT services.				
5.5. IT should form an integral part of the company's risk management	5.5.1 Management should regularly demonstrate to the board that the company has adequate resilience arrangements in place for disaster recovery.	EDM03.01 EDM03.02 EDM03.03	Determine the level of IT-related risk that the enterprise is willing to take to meet its objectives (risk appetite) Evaluate and approve proposed IT risk tolerance thresholds against the enterprise's acceptable risk and opportunity levels. Determine the extent of alignment of the IT risk strategy to enterprise risk strategy.	Promote an IT risk-aware culture and empower the enterprise to proactively identify IT risk, opportunity and potential business impacts Direct the integration of IT risk strategy and operations with the enterprise strategic risk decisions and operations	Monitor the extent to which the risk profile is managed within the risk appetite thresholds.
	5.5.2. The board should ensure that the company complies with IT laws and that IT-related rules, codes are considered.	EDM03.01 EDM03.02 EDM01.03	Determine that IT use is subject to appropriate risk assessment and evaluation, as described in relevant international and national standards.	Direct that risk, opportunities, issues and concerns may be identified and reported by anyone at any time. Risk should be managed in accordance with published policies and procedures and escalated to the relevant decision-makers	Monitor regular and routine mechanisms for ensuring that the use of IT complies with relevant obligations (regulatory, legislation, common law, contractual), standards and guidelines.
	5.6.1. The board should ensure that there is a system in place for management of	EDM04.01 EDM04.02 EDM04.03	Examine and make judgement on the current and future strategy, options for providing IT	Communicate and drive the adoption of resource management strategies,	Monitor the allocation and optimisation of resources in accordance with

5.6. The board should ensure information assets are managed effectively	information which should include information security, information management and information privacy		resources, and developing capabilities to meet current and future needs (including outsourcing). Define the principles for guiding the allocation and management of resources and capabilities so that IT can meet the needs of the enterprise, with the required capability according to the agreed-on priorities and budgetary constraints.	principles, and agreed-on resources plan and enterprise architecture strategies.	enterprise objectives and priorities using agreed-on goals and metrics. Monitor IT sourcing strategies, enterprise architecture strategies, IT resources and capabilities to ensure that current and future needs of the enterprise can be met.
	5.6.2. The board should ensure that all personal information is treated by the company as an important business asset and identified.	EDM04.01 EDM04.02	Understand the key elements of governance required for the reliable, secure and cost-effective delivery of optimal value from the use of existing and new IT services, assets and resources.	Establish principles related to safeguarding resources	
	5.6.3. The board should ensure that an Information Security Management system is developed and implemented.	EDM04.01 EDM04.02	Define principles for the management and control of the enterprise architecture.	Communicate and drive the adoption of the resource management strategies, principles, agreed-on resource plan and enterprise	

				architecture strategies.	
	5.6.4. The board should approve the information security strategy and delegate and empower management to implement the strategy.	EDM04.02		Assign responsibilities for executing resource management.	
5.7. A risk committee and audit committee should assist the board in carrying out its IT responsibilities	5.7.1. The risk committee should ensure that IT risks are adequately addressed.	EDM03.01 EDM03.02 EDM03.03	Proactively evaluate IT risk factors in advance of pending strategic decisions and ensure that risk-aware enterprise decisions are made.	Direct the development of risk communication plans (covering all levels of the enterprise) as well as risk action plans.	Report any risk management issues to the board or executive committee.
	5.7.2. The risk committee should obtain appropriate assurance that controls are in place and effective in addressing IT risks.	EDM03.01 EDM03.02 EDM03.03	Evaluate risk management activities to ensure alignment with the enterprise's capacity for IT-related loss and leadership tolerance of it.	Direct implementation of appropriate mechanisms to respond quickly to changing risk and report immediately to appropriate levels of management, supported by agreed-on principles of escalation (what to report, when, where and how) Identify key goals and metrics of risk governance and management processes to be monitored, and approve the	Monitor the extent to which the risk profile is managed within the risk appetite thresholds. Monitor the key goals and metrics of risk governance and management processes against targets, analyse the cause of the deviation, and initiate remedial action to address the underlying causes.

				approaches, methods, techniques and processes for capturing and reporting the measurement of information.	
	5.7.3. The audit committee should consider IT as it relates to financial reporting and the going concern of the company.	EDM02.01 EDM05.03	Understand and consider how effective current roles, responsibilities, accountabilities and decision-making bodies are in ensuring value creation from IT-enabled investments, services and assets.		Determine whether the requirements of different stakeholders are met.
	5.7.4. The audit committee should also consider the use of technology to improve audit coverage and efficiency.	EDM02.01 EDM05.03			

UNIVERSITY
OF
JOHANNESBURG