Bridging the Information Technology (IT) gap in South Africa through a step by step approach to IT governance

By David Petrus Botha

Presented in partial fulfilment of the requirements for the degree of Master of Commerce (Computer Auditing)

in the

FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES

at

STELLENBOSCH UNIVERSITY

Supervisor: Ms Anria van Zyl

March 2014

Stellenbosch University http://scholar.sun.ac.za

Declaration

I, the undersigned, hereby declare that the work contained in this assignment is my own original work except as indicated in the list of references. I hold all authors' rights to this document and have not previously, in its entirety or in part, submitted this research to this or any other university for a degree. It is submitted in partial fulfilment for the requirements of the degree of Master of Commerce (Computer Auditing) (Stellenbosch University).

1 November 2013

Copyright 2013 Stellenbosch University

All rights reserved

Stellenbosch University http://scholar.sun.ac.za

Acknowledgements

I appreciate the patience of and the contributions made by

- My wife, Andra Botha and
- My supervisor, Anria van Zyl

during the period that I conducted this research.

Stellenbosch University http://scholar.sun.ac.za

Abstract

The focus of this research was to compile a practical, step by step approach that can be followed by those persons charged with the governance of enterprises in South Africa to successfully bridge the information technology gap.

The King Code of Corporate Governance for South Africa and the King Report on Corporate Governance for South Africa (together KINGIII) was identified as a starting point for the compilation of the approach. KINGIII is the corporate governance standard in South Africa and in the introduction to KINGIII it is recommended that the principles contained in the Code should be implemented by all entities. KINGIII is the third report on governance issued by the King Committee and introduced governance principles for Information Technology (IT). The Code contains seven IT governance principles and 24 recommended practices.

The application of the IT governance principles of KINGIII, as well as the related recommended practices, is a complicated endeavour. This is partly because IT in itself is complex and also partly because the governance of IT is a relatively new area of corporate governance.

Through a detailed study of the seven IT governance principles of KINGIII, as well as the related recommended practices and narrative discussions, it was identified that in order to successfully implement IT governance, a company has to establish and implement an IT governance framework which includes relevant **structures, processes and mechanisms** to enable IT to deliver value to the business. It was also identified that the IT governance framework has to facilitate and enhance the company's ability to reach its stated objectives by ensuring that the most appropriate **decisions** are made in respect of the incorporation of IT into the operations of the business. Lastly, it was identified that a company must acquire and use **appropriate technology and people** to support its business.

To address the requirement for the establishment and implementation of relevant **structures, processes and mechanisms**, a framework of 33 IT governance practices was identified, mapped to the IT governance principles of KINGIII and an analysis performed. Through this analysis the IT governance practices that can be utilised to implement the IT governance principles of KINGIII were identified and discussed.

To address the requirement of ensuring that the framework facilitates that the most appropriate decisions are made in respect of the incorporation of IT into the operations of the business, five **key decisions** that have to be made in respect of IT was identified and discussed. The five decisions were mapped to (1) the KINGIII principles to demonstrate which of the IT governance principles are addressed by each of the decisions and (2) the IT governance structures identified in the framework above to demonstrate which of the IT governance structures can be used to provide **input** into taking the relevant decision and which can be used to **take** the decision.

Finally, to address the requirement that a company must acquire and use **appropriate people and technology** to support its business, a framework of organizational competencies required in small and medium-sized enterprises (SME's) was identified and mapped to (1) the KING III principles to demonstrate which of the IT governance principles could be addressed by each of the relevant competencies and (2) to the five key IT decisions identified above to demonstrate which of the competencies can be utilised to make each of the five key decisions.

Based on the findings of the research conducted as set out above, the practical, step by step approach was compiled.

Uittreksel

Die fokus van hierdie navorsing was die samestelling van ‘n praktiese, stapsgewyse benadering wat gebruik kan word deur daardie persone wat verantwoordelik is vir die korporatiewe beheer van ondernemings in Suid Afrika om suksesvol die inligtings tegnologie (IT) gaping te oorbrug.

Die King Code of Corporate Governance for South Africa en die King Report on Corporate Governance for South Africa (gesamentlik KINGIII), was geidentifiseer as ‘n beginpunt vir die samestelling van die benadering. KINGIII is die korporatiewe beheer standaard in Suid Afrika en in die inleiding tot KINGIII word alle ondernemings aanbeveel om die korporatiewe beheer beginsels en gepaardgaande aanbeveelde praktyke te implementeer. KINGIII is die derde verslag oor korporatiewe beheer wat deur die King Komitee uitgereik is en het korporatiewe beheer beginsels met betrekking tot IT bekend gestel. KINGIII bevat sewe koporatiewe beheer beginsels wat met IT verband hou, asook 24 aanbeveelde korporatiewe beheer praktyke.

Die toepassing van die IT korporatiewe beheer beginsels van KINGIII, asook die aanbeveelde praktyke, is ‘n ingewikkelde onderneming. Dit is gedeeltelik omdat IT self kompleks is, maar ook omdat die korporatiewe beheer van IT ‘n relatiewe nuwe area van korporatiewe beheer is.

Deur middel van ‘n in diepte studie van die sewe korporatiewe beheer beginsels van KINGIII, insluitend die aanbeveelde korporatiewe beheer praktyke en besprekings, is daar geïndetifiseer dat ‘n IT korporatiewe beheer raamwerk saamgestel en geimplementeer moet word as deel van die implementering van korporatiewe beheer oor IT. Hierdie IT korporatiewe beheer raamwerk moet relevante **strukture, prosesse en meganismes** bevat wat IT daartoe instaat sal stel om waarde toe te voeg tot die onderneming. Dit is ook geïdentifiseer dat die IT korporatiewe beheer raamwerk die onderneming se vermoeë om sy doelstellings te bereik moet verbeter deur te verseker dat die mees gepaste besluite geneem word met betrekking tot die

integrasie van IT in die bedrywighede van die onderneming. Laastens is daar geïdentifiseer dat ‘n maatskappy toepaslike tegnologie en mense moet bekom en aanwend om die bedrywighede van die onderneming te ondersteun.

Om die vereiste vir die samestelling en implementering van relevante **strukture, prosesse en meganismes** aan te spreek, is ‘n raamwerk van 33 IT korporatiewe beheer praktyke geïdentifiseer, kruisverwys na die IT korporatiewe beheer beginsels van KINGIII en verder ontleed. Deur hierdie ontleding is die IT koporatiewe beheer praktyke wat aangewend kan word om die IT korporatiewe beheer beginsels te implementeer geïdentifiseer en bespreek.

Om die vereiste aan te spreek dat die raamwerk fasiliteer dat die mees gepaste besluite geneem word met betrekking tot die integrasie van IT in die bedrywighede van die onderneming, is vyf **sleutel besluite** wat in verband met IT geneem moet word geïdentifiseer en bespreek. Die vyf besluite is (1) kruisverwys na die IT korporatiewe beheer beginsels van KINGIII om te demonstreer watter IT korporatiewe beheer beginsels deur elke besluit aangespreek word en (2) na die IT korporatiewe beheer strukture wat in die bogenoemde raamwerk geidentifiseer is om aan te dui watter IT korporatiewe beheer strukture gebruik kan word om **insette** te verskaf vir die neem van die vyf sleutel besluite en watter strukture gebruik kan word om die besluite te **neem**.

Laastens, om die vereiste aan te spreek dat ‘n maatskappy **toepaslike tegnologie en mense** moet bekom en aanwend om sy bedrywighede te ondersteun, is ‘n raamwerk van organisatoriese bevoegdhede wat benodig word in klein tot medium-groote ondernemings (SME’s) geïdentifiseer en kruisverwys na (1) die KINGIII korporatiewe beheer beginsels om aan te dui watter IT korporatiewe beheer beginsels deur die relevante bevoegdhede aangespreek word en (2) na die vyf sleutel besluite wat hierbo geïdentifiseer is om aan te dui watter van die bevoegdhede aangewend kan word om elkeen van die vyf sleutel besluite te neem.

Die stapsgewyse benadering tot die korporatiewe beheer van IT is gevolglik saamgestel met verwysing na die bevindinge van die navorsing wat uitgevoer is soos hierbo uiteengesit.

Stellenbosch University http://scholar.sun.ac.za

Table of contents

Stellenbosch University http://scholar.sun.ac.za

1. Chapter 1: Introduction

1.1 Background

The King Report on Governance for South Africa 2009 (the Report) and the King Code of Governance for South Africa 2009 (the Code) (collectively referred to in this document as KINGIII) was issued in September 2009 and became effective on 1 March 2010 (IODSA, 2009a; IODSA, 2009b).

KINGIII is the third report on governance compiled by the King Committee. As explained in KINGIII, the revised report became necessary because of the new South African Companies Act no. 71 of 2008 (the Act) and changes to international governance trends.

The Report and Code introduced principles and recommended practices for the governance of Information Technology (IT).

The Code sets out seven IT governance principles as well as 24 recommended practices that the board and / or management of a company should follow to address the seven principles of IT governance.

KINGIII recommends that all entities should apply the principles and recommended practices therein and by doing so, achieve good governance (IODSA, 2009a:17).

In terms of paragraph 3.84 of the listing requirements of the Johannesburg Stock Exchange (JSE) (JSE Limited, 2011:47), companies listed on the JSE must comply with the corporate governance requirements of KINGIII.

There is however no legal requirement for South African companies that are not listed on the JSE to comply with the principles of corporate governance set out in KINGIII.

Certain of the corporate governance requirements of KINGIII have been included in the Act and apply to certain South African companies which are not listed on the JSE when certain specific requirements are met. These requirements are set out in Chapter 3 of the Act and include the establishment of an audit committee.

In the introduction and background section to KINGIII (IODSA, 2009a:6), the link between governance principles and law is explained. Firstly, it is argued that the directors and officers of a company have a duty to discharge their legal duties. These duties are grouped into two categories, namely (1) the duty of care, skill and diligence and (2) fiduciary duties. It is further argued that the criteria of good governance will become important when determining what is regarded as an appropriate standard of conduct for directors. The more established these governance practices become, the more likely it is that a court will come to a conclusion that conduct conforming with these practices meet the required standard of care. Finally, it is argued that any failure to comply with a recognised standard of governance may render a board, or an individual director, legally liable, even if it has not been legislated.

In the context of the above, it seems that the directors and officers of a company should at least consider applying the principles of KINGIII, as well as the related recommended practices, in order to manage their personal risk, as well as the risk of the board. In instances where the application of the principles or recommended practices is not found to be practical or not to add value, the reasons for this conclusion should be documented for future reference (IODSA, 2009a:16).

There are however other, more positive reasons why the principles of corporate governance should be applied by the board and / or management of all companies.

In COBIT 5, a recognised framework for IT governance, it is explained that the main objective of governance is value creation. The objectives supporting this main objective are (1) benefits realisation, (2) risk optimisation and (3) resource optimisation (ISACA, 2012:17). Gartner (2012a) found that where governance is driven from a corporate objectives perspective, the result is better business outcomes delivered through the governance process. According to Gartner, the three

business outcomes which are important to most businesses include (1) top-line growth (or value creation), (2) operational excellence (or resource optimisation) and (3) risk optimisation (or risk optimisation).

Governance is therefore focussed on creating value for stakeholders of the enterprise by the realisation of benefits through the optimal utilisation of resources at an acceptable level of risk.

Once the decision has been made to apply the KINGIII principles for IT governance, as well as the recommended practices, the board and / or management have to put this decision into action.

From an analysis of the Code, it is not always that clear what exactly the board and / or management should do to implement the decision to apply the principles of IT governance. Pertinent questions that may have to be answered could include:

- **What** exactly is IT governance? **What** does it consist of?
- **How** can the technology components (or parts) relating to IT be identified?
- **Who** should govern IT? **How** should it be governed? **What** should be done to govern IT?
- **Who** should manage IT? **How** should it be managed? **What** should be done to manage IT?
- **Who** should identify the risks relating to IT? **How** should these risks be identified?

The questions set out above mainly relate to ***who*** should take responsibility and accountability for a certain aspect of the governance or management of IT, ***how*** it can (or should) be governed or managed and ***what*** should be done to govern or manage IT.

The principles in KINGIII set out, at a high level, ***who*** should take responsibility for the governance and management of IT, as well as ***what*** should be done, but it does not address in detail ***how*** it should be done.

Fortunately, a large amount of research has been conducted in this respect, which can be utilised to compile a step by step approach that the directors and / or management of a company can follow to successfully implement IT governance as envisaged in KINGIII.

1.2 Research objective and value of the study

The objective of this research is to **compile** a **practical**, **step by step** approach that can be used by those persons charged with the **governance and / or management** of **medium sized enterprises** in **South Africa**, to **enable** them to successfully **bridge the IT gap**.

From the discussion under the Background section above, it is clear that once the board has decided to apply the principles and recommended practices of corporate governance as set out in KINGIII, the implementation thereof could proof challenging.

In the context of IT governance it may be even more complex, as IT by its nature is complex and dynamic. According to Weill and Ross (2004b:1), IT governance is a mystery to key decision makers at most companies. The board and business management and staff may not understand IT and the IT management and staff may not understand the principles of governance and the business as a whole. This lack of understanding results in a **gap** between the business and IT which is referred to as the **IT gap**. The IT gap can amongst other things lead to the misalignment of the business and IT. It is this misalignment that has to be addressed as required by IT governance principle two of KINGIII (IODSA, 2009a:82).

The boards and management of companies, who have decided to implement the principles of IT governance set out in KINGIII, should benefit from the results of this study, as the approach should enable them to approach the implementation of IT governance in a structured manner. This should enhance their chances of a successful implementation.

1.3 Research design and methodology

This research is based on a non-empirical study. Literature relating to the governance of IT was reviewed, with specific focus on literature that relates to the seven IT governance principles and 24 recommended practices set out in KINGIII. A practical approach to IT governance was compiled based on the literature review and analysis.

In chapter 2, the seven IT governance principles of the Code is analysed and discussed in the context of the 24 recommended practices and detailed narrative discussions in KINGIII, together with other relevant literature on IT governance. The concepts of (1) governance, (2) information, (3) information technology, (4) principles, (5) practices and (6) policies were defined and the following concepts relating to IT governance identified:

- IT governance structures, processes and mechanisms.
- Five key IT questions that have to be addressed by the board and management.
- Appropriate technology, processes and people to support the business and its governance requirements.

Building on the findings of chapter 2, chapter 3 introduces the concept of access paths and proposes its use for the documentation and analysis of the IT environment. The concepts identified in chapter 2 are discussed and analysed in the context of relevant literature. From the analyses performed, structures, processes and mechanisms are identified which can be approved and implemented to apply the IT governance principles of KINGIII. The five key IT decisions that have to be addressed by the board and management are discussed and brought into relation with IT governance structures that can be utilised to provide input to and / or take the relevant decisions. Lastly, competences that can be utilised to address the IT governance principles of KINGIII and the key IT decisions are discussed and analysed.

Chapter 4 concludes by setting out the proposed step by step approach for the implementation of IT governance, based on the findings contained in chapters 2 and 3.

1.4 Scope and limitations of the study

The research is subject to the following limitations:

- The approach has been formulated based on the IT governance principles of KINGIII, which is the governance standard in South Africa. The approach may therefore not be appropriate for the implementation of IT governance in other jurisdictions.
- The approach has been compiled based on an analysis of the IT governance principles of KINGIII, as well as other relevant literature on IT governance, and has not been tested in practice. As a result, there is an opportunity to follow the approach in practice to determine to what extent the approach assists those charged with the governance of organization's to successfully apply the IT governance principles of KINGIII.
- The approach is not directed to a specific type of business or a specific industry, but has been compiled to be sufficiently generic to be used by all companies who have decided to implement the IT governance principles of KINGIII.

2. Chapter 2: Review and discussion of the Information Technology ('IT') governance principles of KINGIII

2.1 Introduction to Chapter 2

The King Committee issued two documents in September 2009, namely the King Report on Governance for South Africa 2009 (the Report) and the King Code of Governance for South Africa 2009 (the Code) (IODSA, 2009a; IODSA, 2009b).

The Report contains nine chapters and narrative discussions on all the principles of corporate governance contained in the report. The Code has nine sections and sets out the governance principles contained in the Report as well as related recommended practices in a tabular format.

KINGIII suggests that all entities should apply the corporate governance principles which are set out in the Code and consider implementing the best practice recommendations contained in the Report (IODSA, 2009a:17).

Chapter 5 of the Report, and section 5 of the Code, addresses the governance of IT. The Code sets out seven IT governance principles and 24 recommended practices. A summary of the seven principles and the related recommended practices are set out in Table 1.

The purpose of this chapter is to discuss the seven IT governance principles of the Code, in the context of the recommended practices and detailed narrative discussions in KINGIII, as well as other relevant literature on IT governance.

The discussion of the seven IT governance principles in this chapter will form the context for the identification and discussion of ***how*** the board and / or management can successfully apply the IT governance principles of KINGIII.

Table 1: KINGIII IT governance principles and recommended practices

Principle (P)	Recommended practice/(s) (RP)
P1: the board should be responsible for IT governance	**RP1:** the board should assume responsibility for the governance of IT and place it on the board agenda.
	RP2: the board should ensure that an IT charter and policies are established and implemented.
	RP3: the board should ensure promotion of an ethical culture and awareness and a common IT language.
	RP4: the board should ensure that an IT internal control framework is adopted and implemented.
	RP5: the board should receive assurance on the effectiveness of the IT internal controls.
P2: IT should be aligned with the performance and sustainability objectives of the company	**RP6:** the board should ensure that the IT strategy is integrated with the company's strategic and business processes.
	RP7: 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.
P3: the board should delegate to management the responsibility for the implementation of an IT governance framework	**RP8:** management should be responsible for the implementation of the structures, processes and mechanisms for the IT governance framework.
	RP9: the board may appoint an IT steering committee of similar function to assist with its IT governance.
	RP10: the CEO should appoint a Chief Information Officer ('CIO') responsible for the management of IT.
	RP11: the CIO should be a 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.
P4: the board should monitor and evaluate significant IT investments and expenditure	**RP12:** the board should oversee the value delivery of IT and monitor the return on investment from significant IT projects.
	RP13: the board should ensure that intellectual property contained in information systems is protected.
	RP14: the board should obtain independent assurance on the IT governance and controls supporting outsourced IT services.
P5: IT should form an integral part of the company's risk management	**RP15:** management should regularly demonstrate to the board that the company has adequate business resilience arrangements in place for disaster recovery.
	RP16: the board should ensure that the company complies with IT laws and that IT related rules, codes and standards are considered.
P6: the board should ensure that information assets are managed effectively	**RP17:** the board should ensure that there are systems in place for the management of information which should include information security, information management and information privacy.
	RP18: the board should ensure that all personal information is treated by the company as an important business asset and is identified.

	RP19: the board should ensure that an Information Security Management system is developed and implemented.
	RP20: the board should approve the information security strategy and delegate and empower management to implement the strategy.
P7: a risk committee and audit committee should assist the board in carrying out its IT responsibilities	**RP21:** the risk committee should ensure that IT risks are adequately addressed.
	RP22: the risk committee should obtain appropriate assurance that controls are in place and effective in addressing IT risks.
	RP23: the audit committee should consider IT as it relates to financial reporting and the going concern of the company.
	RP24: the audit committee should also consider the use of technology to improve audit coverage and efficiency.

Source: IODSA (2009b:39 – 41)

2.2 Defining certain important terms

In order to understand the principles and recommend practices set out in KINGIII, it is useful to understand the concepts of **governance, information, information technology (IT), principles, practices and policies.**

Gartner (2012b), defined **governance** as "the process of:

- Setting decision rights and accountability, as well as establishing policies that are aligned to objectives.
- Balancing investments in accordance with policies and in support of business objectives.
- Establishing measures to monitor adherence to decisions and policies.
- Ensuring that processes, behaviours and procedures are in accordance with policies and within tolerances to support decisions."

"**Information** is raw data that has been verified to be accurate and timely, is specific and organised for a purpose, is presented within a context that gives it meaning and relevance and which leads to an increase in understanding and a decrease in uncertainty" (IODSA, 2009a:119).

"**Information technology** (IT) is the collective term for the various technologies involved in processing and transmitting information. They include computing,

telecommunications, and microelectronics. The term became popular in the UK after the Government's "Information Technology Year" in 1972" (Collins, 2006).

A **principle**, according to the definition contained in COBIT 5 (ISACA, 2012:92), is an "enabler of governance and management. It comprises the values and fundamental assumptions held by the enterprise, the beliefs that guide and puts boundaries around the enterprise's decision making, communication within and outside the enterprise, and stewardship – caring for assets owned by another."

Good practice, as defined in COBIT 5 (ISACA, 2012:92), is a "proven activity or process that has been successfully used by multiple enterprises and has shown to produce reliable results."

A **policy**, is defined in COBIT 5 (ISACA, 2012:92), as an "overall intention and direction as formally expressed by management."

2.3 Principle 1: The board should be responsible for IT governance

KINGIII defines **responsibility** as "the state or position of having control or authority and being accountable for ones actions and decisions" (IODSA, 2009a:122).

Good corporate governance is described in KINGIII as essentially being about effective and responsible leadership. The characteristics of responsible leadership include the ethical values of responsibility, accountability, fairness and transparency (IODSA, 2009a:20).

By assuming responsibility for the governance of IT, the board therefore takes control over the leadership of IT and accepts responsibility and accountability for actions taken, and decisions made, in respect of IT in the enterprise.

Weill and Ross (2004b:14 – 18) identified a number of reasons why the governance of IT is important. Seven of these reasons are summarised in Table 2.

Table 2: Reasons why IT governance is important

Reason	Discussion
Good IT governance pays off	Weill and Ross identified that enterprises with above average governance performance generated return on assets of more than twenty percent higher than enterprises with poor governance performance; with all the firms considered pursuing a similar business strategy.
IT is expensive	Weill and Ross identified that the annual investment of enterprises in IT is growing and as IT has become more important and pervasive, senior management is increasingly challenged to manage and control IT to ensure value is created.
IT is pervasive	Weill and Ross found that the central management of IT is no longer possible or desirable. IT spending now originates all over the enterprise and well-designed governance arrangements distribute IT decision making to those responsible for specific outcomes.
New IT opportunities bombard enterprises with new business opportunities	New technologies, including Web-based services, mobile technologies and enterprise systems are introduced at a rapid pace and can create strategic threats and / or new opportunities. IT infrastructure should therefore balance the dual needs of cost effectiveness in meeting current business needs and flexibility to adapt to and support future business needs.
IT governance is critical to organizational learning about IT value	Effective IT governance creates mechanisms through which enterprises can debate the potential value of IT investments. Formal exception processes are established and enterprises can learn through these exceptions and share new practices identified across the enterprise, if appropriate.
IT value depends on more than good technology	Weill and Ross found that the implementation failure of large IT investments, mostly related to an inability of the organizations to effectively adopt new business processes that apply the new technologies. They also found that as the implementation of new IT solutions enable increasing standardisation and integration of business processes, the roles of IT technical staff and business leaders become more and more intertwined.
Senior management has limited bandwidth	Senior management cannot make all the IT related decisions throughout the enterprise as they simply do not have the time available to do so. Carefully designed IT governance provides for clearly defined and transparent IT decision making processes, which ensures that managers throughout the enterprise make IT decisions that are in line with the overall direction of senior management.

Source: Weill and Ross (2004b: 14 – 18)

Gartner (2009:1) found that IT governance must be driven by corporate governance and that professional investors are willing to pay more for companies with strong and effective corporate governance.

KINGIII requires that the board should adopt an IT governance framework which includes relevant **structures, processes and mechanisms** which will enable IT to deliver the required value to the company and to mitigate risk to an appropriate level (IODSA, 2009a:82).

The IT governance framework should be appropriate and applicable to the company and should facilitate and improve the company's ability to achieve its objectives by taking the most appropriate **decisions** about how to incorporate IT into its operations (IODSA, 2009a:82).

The concepts of **structures, processes and mechanisms** will be discussed and analysed in more detail in chapter 3.

The **decisions** that have to be taken in respect of IT will also be identified and discussed in chapter 3.

2.4 Principle 2: IT should be aligned with the performance and sustainability objectives of the company

The alignment of the IT strategy with the overall strategy of the enterprise is a widely supported concept and is the second IT governance principle set out in KINGIII.

According to the IT Governance Institute (2003:11) the purpose of IT governance includes the objective of the alignment of IT with the business and the realisation of the planned benefits.

Byrd, Lewis and Bryan (2006:315) found that strategic alignment in small and medium-sized manufacturing enterprises resulted in the leveraging of those enterprises' IT investments. The enterprises could increase their revenue and profits

by better aligning their IT and business strategies without increasing their investments in IT.

A number of authors have conducted research on the alignment of IT strategy and business strategy. Chen, Sun, Helms and Jih (2008:366) stated that researchers agree that strategic alignment is the most significant issue facing IT. Cragg, King and Hussein (2002:109) conducted a study focussed on the alignment between the business strategy and IT strategy among small UK manufacturing firms. De Haes and Van Grembergen (2009:123) found that the maturity of business and IT alignment is higher when organizations use a mix of mature IT governance practices. Weill and Ross (2004a) indicated that managers of enterprises are increasingly aware that IT-related decisions and processes must be aligned with the organization's overall performance goals. Further to this, Gartner (2011) found that coherent action by all the various parts of a business could give a competitive advantage to organizations. Their findings indicated that coherent action requires the organization's resources and activities to support the strategy which has been approved by the board and that strategies which have not been approved should not be awarded any resources at all.

From the above it is clear that the alignment of the IT strategy of an enterprise with its business strategy is extremely important and that IT governance plays an important role in ensuring that the process of alignment is put into motion.

The principle of alignment and the mechanisms available to facilitate alignment will be discussed in more detail in chapter 3.

2.5 Principle 3: The board should delegate to management the responsibility for the implementation of an IT governance framework

This principle in essence requires the board to instruct management to implement an appropriate IT governance framework.

The fifth principle in COBIT 5 makes a clear distinction between governance and management (ISACA, 2012:14). In COBIT 5, **governance** is described as ensuring that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives that have to be achieved, setting the direction of the enterprise through prioritisation and decision making and monitoring performance and compliance against agreed-on direction and objectives (ISACA, 2012:14).

As explained in COBIT 5, "**management** plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives" (ISACA, 2012:14).

KINGIII also draws this distinction between governance and management. Generally, the board must assume certain responsibilities, ensure that certain things are done, receive assurance in certain instances, delegate certain responsibilities and oversee certain activities, but the board is never required to implement anything at an executive level. This is in line with the definition of governance in KINGIII, which describes governance as essentially being responsible and effective leadership (IODSA, 2009a:20).

The management of an enterprise should implement structures, processes and mechanisms which are required, in the context of the specific enterprise, to successfully implement the adopted IT governance framework (IODSA, 2009a:83).

De Haes and Van Grembergen (2008:445) conducted a study to determine the minimum baseline of structures, processes and relational mechanisms which should be implemented by all enterprises as part of their implementation of IT governance. The findings of this study and its application in terms of the requirements of KINGIII will be discussed in more detail in chapter 3.

2.6 Principle 4: The board should monitor and evaluate significant IT investments and expenditure

"The company should ensure that it acquires and uses appropriate technology, processes and people to support its business and governance requirements in a timely manner and accurately" (IODSA, 2009a:84).

As discussed under principle 1 above, IT is expensive. KINGIII therefore requires that the board oversee the value delivery of IT and ensure that the return on investment from significant IT investments is delivered as promised (IODSA, 2009a:84).

The IT Governance Institute describes value delivery as "concentrating on optimising and proving the value of IT" (ITGI, 2003:24). They also explain that for the required IT value delivery to be achieved, both the return on investment and the actual costs of IT have to be managed appropriately.

2.7 Principle 5: IT should form an integral part of the company's risk management

KINGIII requires that IT risks should be identified and managed as part of a company's overall risk management activities, as required by chapter 4 of the Report (IODSA, 2009a:85).

The Report, under the IT governance chapter, specifically highlights IT legal risk, which is explained as arising from the possession, ownership or operational use of technology on an illegal basis (IODSA, 2009a:85). The boards should ensure that, in the context of IT legal risk, relevant IT related laws, rules and codes are considered as part of the management of these risks.

KINGIII also requires that the board consider the use of IT in managing the other risks of the company, including compliance with laws and regulations (IODSA, 2009a:85).

The IT Governance Institute (2003:26) includes technology risk and information security risk as part of IT risk management. In addition to this, the IT Governance Institute recommends that boards should manage enterprise risk by:

- Ensuring that there is *transparency* about significant risks and clarifying the risk-taking or risk-avoidance policies of the enterprise;
- Understanding that the *responsibility* for risk management rests with the board, even if the responsibility is delegated to management;
- Understanding that the system of internal control which is put in place to manage risks can often generate *cost-efficiencies*;
- Understanding that a transparent and pro-active approach to risk management can create *competitive advantage* for the organization;
- Ensuring that risk management is embedded into the operations of the organization.

In respect of risks that have been identified, the IT Governance Institute indicates that the board and management may choose to:

- **Mitigate** the risk – implement controls to manage the risk;
- **Transfer** the risk – share the risk with a partner or take out insurance to manage the risk;
- **Accept** the risk – acknowledge the risk and monitor it, but do nothing more to manage the risk.

As a minimum, risks should therefore at least be identified and analysed, and a conscious decision taken on how to address (or not address) the identified risk (ITGI, 2003:27).

2.8 Principle 6: The board should ensure that information assets are managed effectively

The sixth IT governance principle of KINGIII relates to the management of information.

In terms of KINGIII the formal process to manage information includes (1) information management, (2) information privacy and (3) information security (IODSA, 2009a:86).

In relation to the management of information, KINGIII requires the board to ensure that there are systems in place for the management of information assets and for the performance of certain data functions. Information records are viewed as the most important information assets of a business as it provides evidence of business activities (IODSA, 2009a:86).

KINGIII requires the board to ensure that there are systems in place to identify and safeguard personal information that is processed and retained by the company. Laws relating to personal information should be considered and adhered to (IODSA, 2009a:86).

An information security management system should be developed and implemented by the board and management respectively. This system should ensure the (1) confidentiality, (2) integrity and (3) availability of information systems and information on a timely basis (IODSA, 2009a:87).

2.9 Principle 7: A risk committee and audit committee should assist the board in carrying out its IT responsibilities

This principle requires the establishment of an audit committee and a risk committee to assist the board with its IT governance responsibilities (IODSA, 2009a:87).

The audit committee should be responsible for IT to the extent that it relates to the financial reporting and going concern aspects of the company. This committee should also consider the use of IT to improve audit coverage and efficiency (IODSA, 2009a:87).

The risk committee should ensure that IT risks are identified and adequately addressed as part of the company's overall risk management process. This committee should understand the company's overall exposure to IT risks, including the areas of the business that are most dependent on IT for their continued effective operation (IODSA, 2009a:87).

2.10 Conclusion of Chapter 2

The purpose of this chapter was to review and discuss the seven IT governance principles of KINGIII in the context of the recommended practices and detailed narrative discussions contained in the Report and the Code, as well as other relevant literature in respect of IT governance.

The concepts that have been identified in this chapter and which will be discussed in more detail in chapter three include the following:

- In terms of principle one, the board of a company is required to assume responsibility for the governance of IT. In chapter 3 under section 3.2, the concept of an **access path** will be introduced as a method of identifying the IT assets of a company which can be used to gain an understanding of the IT environment which has to be governed.

- Under principle one it was identified that an IT governance framework should be adopted by the board. It was also identified that the IT governance framework should include relevant **structures, processes and mechanisms** which will enable the successful implementation of such a framework. In terms of principle three it is clear that management is responsible for the implementation of the IT governance framework. The concepts of **structures, processes and mechanisms** will be discussed in chapter 3 under section 3.3.

- Principle one also requires that the IT governance framework should facilitate and improve the company's ability to reach its objectives by making the most appropriate **decisions** about how to incorporate IT into the operations of the

business. The five major decisions that have to be taken in respect of IT will be identified and discussed in chapter 3 under section 3.4.

- Finally, under principle four it was identified that a company should ensure that it acquires and uses appropriate technology, processes and people to support its business and governance activities. Specific IT **competences** required in respect of small to medium-sized enterprises will be discussed in chapter 3 under section 3.5.

3. Chapter 3: Identification and discussion of *how* the board and / or management can successfully apply the IT governance principles of KINGIII

3.1 Introduction to Chapter 3

The purpose of this chapter is to identify and discuss ***how*** the principles of IT governance can be implemented in practice.

Firstly, the concept of **access paths** will be introduced and discussed as a method that can be used to analyse the IT environment which has to be governed and managed by the board and management respectively. Thereafter, various **structures, processes and relational mechanisms** which can be approved by the board and implemented by management will be identified and discussed. Thirdly, the five **key IT decisions** that have to be addressed and structures available to facilitate taking these decisions will be identified and discussed. Lastly, the chapter will include a discussion on the acquisition and maintenance of relevant **competences** which are required to govern and manage IT.

3.2 Analysis of the IT environment through the utilisation of access paths

The first principle of IT governance requires the board to assume responsibility for the governance of IT (IODSA, 2009a:82). It also requires that the company should understand IT, including the benefits, risks and constraints relating to IT.

Information and the **technologies** that are/can be utilised to collect, organize, process, store and transmit information (collectively referred to in this research as IT assets), are key assets to any enterprise in the same manner as human assets, financial assets, physical assets, intellectual property and relationship assets (Weill & Ross, 2004b:6).

Although firms manage all these assets, IT assets perplex them the most. As a result, many managers abdicate their responsibilities for ensuring that IT assets are used effectively (Weill & Ross, 2004b:1). The identification and analysis of access paths can be used to document and develop an understanding of the IT environment which has to be governed and managed.

An access path is formed by the various components that need to be activated or utilised in order for a typical user's request to be executed (Boshoff, 1990:24). Boshoff formulated this concept as part of the development of the Path Context Model (PCM) which can be utilised to address computer security in non-secure IT environments.

An access path can be further explained as follows. User A requires access to file F which is located on server S. All the technology components that have to be activated or utilised for user A to obtain access to file F forms the access path between user A and file F (Boshoff, 1990:24 – 25).

Boshoff (1990:41) found that the simplicity of the PCM, which incorporates the concept of access paths, made the use of the model especially effective in complex computer environments. Goosen (2011:33 – 34) successfully utilised the concept of access paths in the development of an integrated framework to align business imperatives with IT governance principles.

As access paths were developed and successfully utilised by Boshoff (1990) to address security in complex IT environments and Goosen (2011) successfully utilised the concept of access paths in the development of an integrated IT governance framework, it is proposed that the concept of access paths can also be utilised to analyze the IT environment and identify the IT assets which is subject to the governance and management of the board and management.

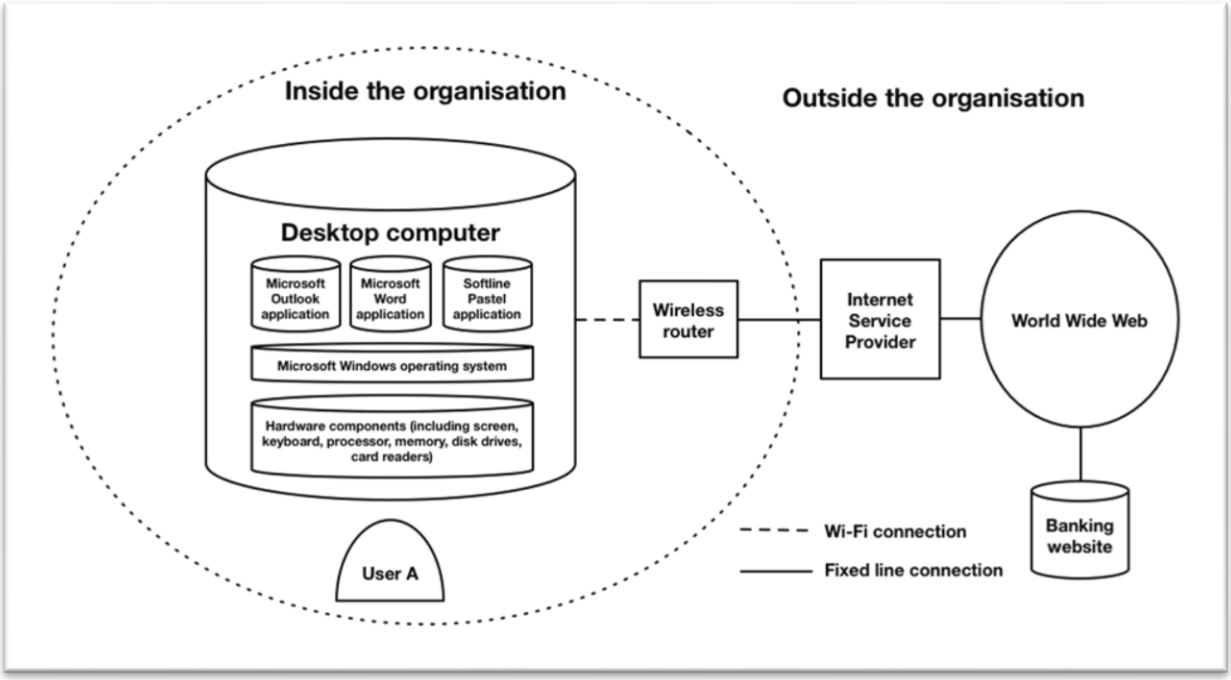
The following example illustrates the utilisation of the concept of an access path:

In this example, user A requires access to internet banking facilities. The access path formed between user A and the banking website is illustrated in Figure 1.

The various components in the access path formed between user A and the banking website can be described as follows:

- Technology component (TC) 1 is the hardware components needed to access the application software required to access the banking website.
- TC2 is the operating system required to operate the desktop computer; in this example Microsoft Windows.
- TC3 is the software application required to access the World Wide Web; in this instance Microsoft Outlook.
- TC4 is the wireless router which is required to connect the desktop computer to the fixed line connection through a Wi-Fi connection.
- TC5 is the fixed line which is required to connect the wireless router to the Internet Service Provider.
- TC6 is the World Wide Web to which access is required to finally access the Banking website.
- TC7 is the banking website which user A would like to access to process certain banking transactions.

Figure 1: Illustration of an access path



(Authors own)

It is proposed that the use of the concept of access paths to analyse and document the IT environment will assist the board and management to obtain a clear understanding of the IT environment which they have to govern and manage.

3.3 Identify and implement relevant structures, processes and relational mechanisms for the governance and / or management of IT

In terms of IT governance principle one included in KINGIII, the board should ensure that an IT governance framework, including relevant structures, processes and mechanisms is established and implemented (IODSA, 2009a:82).

IT governance principle three requires the board to delegate the implementation of the IT governance framework to management (IODSA, 2009a:83).

A significant amount of research has been performed by De Haes and Van Grembergen in respect of IT governance and the practices used to successfully implement IT governance.

De Haes and Van Grembergen (2004) published an article with the main objective being to contribute to the understanding of IT governance and how it can be achieved in practice. The article defined IT governance and identified structures, processes and relational mechanisms which can be used to deploy IT governance.

In 2008, they published an article building on their prior research, with one of the goals being to determine which IT governance best practices are (or can be) used in practice to successfully implement IT governance (De Haes & Van Grembergen, 2008:444). In this research, they highlighted the fact that IT governance is situated in multiple layers in the organisation. These include (1) the strategic level where the board of directors are involved, (2) the management level where the executive management (CEO, CFO, CIO, etc.) are involved and (3) the operational level where IT and business management are involved (De Haes & Van Grembergen, 2008:445).

Through a combination of literature and pilot case research, as well as Delphi research, De Haes and Van Grembergen (2004:449) developed a validated list of IT governance practices that are (or can be) used in practice to implement IT governance.

KINGIII requires the board to ensure that relevant structures, processes and mechanisms are implemented and that management should implement these structures, processes and mechanisms. The validated list of IT governance practices compiled by De Haes and Van Grembergen was mapped to the IT governance principles of KINGIII to determine which of the IT governance practices could be implemented to address the IT governance principles of KINGIII. The table setting out the mapping is included as Appendix A: De Haes and Van Grembergen (2008:449) validated list of IT governance practices mapped to the IT governance principles of KINGIII (IODSA, 2009a).

The mapping of the IT governance practices identified and validated by De Haes and Van Grembergen (2004) and the IT governance principles contained in KINGIII (IODSA, 2009a) as set out in Appendix A, was further analysed to determine which of the IT governance practices are more relevant for organizations who specifically want to apply the IT governance principles of KINGIII. The result of this further analysis is included as Table 3.

To arrive at the result set out in Table 3, the IT governance principles of KINGIII, as well as the related recommended practices and narrative discussions, were analysed to determine (1) to what extent each of the IT governance practices identified and validated by De Haes and Van Grembergen (2004) could be utilised to directly and indirectly address the IT governance principles of KINGIII and (2) to determine to what extent each specific IT governance practice is referred to (directly or indirectly) in KINGIII.

Table 3: Analysis of IT governance (ITG) practices to implement the IT governance principles of KINGIII

De Haes and Van Grembergen (2008:449) validated list of ITG practices			**Count of P**	**Count of S**	**Count of K3**	**SUM of P; S; K3**
S, P or M	#	**Description** of ITG structure, process or relational mechanism				
P	1	IT governance framework COBIT	5	2	3	10
S	2	(IT) audit committee at level of board of directors	2	4	2	8
P	3	Strategic information systems planning	**3**	**3**	**1**	**7**
S	4	IT expertise at level of the board of directors	6	0	0	6
M	5	IT leadership	**4**	**1**	**1**	**6**
S	6	CIO on executive committee	**3**	**2**	**1**	**6**
S	7	CIO reporting to CEO and/or COO	**3**	**2**	**1**	**6**
P	8	IT governance assurance and self-assessment	2	4	0	6
S	9	IT strategy committee at level of board of directors	**5**	**0**	**0**	**5**
S	10	IT steering committee (IT investment evaluation / prioritisation at execution / senior management level)	**3**	**1**	**1**	**5**
S	11	ITG function / officer	2	3	0	5
S	12	Integration of governance / alignment tasks in roles & responsibilities	2	3	0	5
P	13	Portfolio management (incl. business cases, information economics, ROI, payback)	**2**	**2**	**1**	**5**
P	14	Service level agreements	1	4	0	5
M	15	ITG awareness campaigns	1	4	0	5

P	16	IT budget control and reporting	**3**	**1**	**0**	**4**
P	17	IT performance measurement (e.g. IT balanced scorecard)	2	2	0	4
S	18	IT security steering committee	2	1	1	4
P	19	Project governance / management methodologies	**2**	**1**	**1**	**4**
S	20	IT project steering committee	**1**	**3**	**0**	**4**
S	21	Architecture steering committee	1	3	0	4
P	22	COSO / ERM	1	3	0	4
M	23	Corporate internal communication addressing IT on a regular basis	0	4	0	4
M	24	Information meetings between business and IT executives / senior management	3	0	0	3
M	25	Executive / senior management giving the good example	2	1	0	3
M	26	Job-rotation	1	2	0	3
M	27	Co-location	1	2	0	3
M	28	Cross-training	1	2	0	3
M	29	Knowledge management (on ITG)	1	2	0	3
M	30	Business / IT account management	1	2	0	3
S	31	Security / compliance / risk officer	1	1	0	2
P	32	Charge back arrangements – total cost of ownership (e.g. activity based costing)	1	1	0	2
P	33	Benefits management and reporting	1	1	0	2

In Table 3 the following symbols or headings have the following meaning/(s):

- S, P or M refers to IT governance structures, processes and relational mechanisms respectively. Together, these concepts are referred to as IT governance practices.
- # refers to the ranking of the IT governance practice, based on the mapping of the IT governance practices to the IT governance principles of KINGIII.
- Count of P indicates the number of IT governance principles of KINGIII for which the IT governance practice can be utilised to directly address the related IT governance principle.
- Count of S indicates the number of IT governance principles of KINGIII for which the IT governance practice can be utilised to **in**directly address the related IT governance principle.
- Count of K3 indicates the number of times the specific IT governance practice is referred to (directly or indirectly) in KINGIII.
- Sum of P; S; K3 is the mathematical aggregate of Count P, Count S and Count K3.

- The table was sorted based on the Sum of P; S; K3, then Count of P, then Count of S and finally Count of K3.

The following **conclusions** can be drawn from the results of the analysis set out Table 3, specifically in respect of the **top ten** IT governance practices identified through the analysis:

- An **IT governance framework**, such as COBIT 5 (ISACA, 2012), can be utilised to address five of the seven principles of IT governance directly and two indirectly. KINGIII also makes reference to an IT governance framework three times.

  This finding is in line with the findings of De Haes and Van Grembergen (2008:452) which indicated that the effectiveness of an IT governance framework (such as COBIT) as an IT governance practice is high. They did however identify that it is more difficult to implement an IT governance framework such as COBIT, when compared to many of the other IT governance practices. COBIT 5 is a comprehensive IT governance framework that can be implemented by enterprises to assist them in achieving their objectives for the governance and the management of IT (ISACA, 2012:13).

  Gartner (2012:1) reported that COBIT 5 is a significant update from the previous COBIT framework (COBIT 4.1) and now includes other ISACA frameworks which have been integrated into COBIT 5, such as Val IT and Risk IT. They also reported that these changes have made COBIT 5 an even wider reaching and more complex IT governance framework and that the scope of the framework and the related guidance could overwhelm users and inhibit the adoption thereof.

  The COBIT 5 framework is based on five key principles for the governance and management of IT, which include (1) meeting stakeholder needs, (2) covering the enterprise end to end, (3) applying a single integrated framework, (4) enabling a holistic approach and (5) separating governance from management (ISACA, 2012:14).

The principles of COBIT 5 align with all the IT governance principles of KINGIII and the implementation of this governance framework should therefore enable a company to successfully apply all the KINGIII IT governance principles.

- An (IT) **audit committee** at the level of the board of directors can be successfully utilised to directly address two of the seven IT governance principles and four indirectly. An audit committee is also referred to twice in KINGIII. IT governance principle seven specifically requires an audit committee to assist the board with IT governance by considering IT as it relates to financial reporting and the going concern of a company and to the efficiency of audits and audit coverage (ISACA, 2009:87).

- **Strategic information systems planning** is a formal IT governance process with the objective to define and update the IT strategy. It can be utilised to directly address three IT governance principles and three indirectly. The process relates to the alignment of the IT strategy with the business strategy. The importance of the alignment of the IT strategy of an enterprise with the overall business strategy is widely accepted (Byrd et al., 2006:308; Chen et al., 2008:366; Cragg et al., 2002:109; Gartner, 2006:2; ITGI, 2003:22; De Haes & Van Grembergen, 2009:123; IODSA, 2009:83; Luftman, Rapp & Brier, 1999:4).

- **IT expertise at the level of the board of directors** is a structural IT governance practice and can directly address six of the seven IT governance principles of KINGIII. De Haes and Van Grembergen (2008:452) found that although the effectiveness of this IT governance practice is high, it is very difficult to implement and may therefore not be a practical IT governance practice to utilise. This specific IT governance practice is also not specifically referred to in KINGIII.

- **IT leadership** as an IT governance relational mechanism, can be utilised to address four of the IT governance principles directly and one indirectly. This IT governance practice relates to the ability of the CIO to clearly define and explain the vision of IT's role in the organization and to ensure that managers throughout

the organization clearly understands this vision (De Haes & Van Grembergen, 2008:449). KINGIII, under IT governance principle three, requires the CIO to serve as a bridge between IT and the business, which is in line with the objectives of this IT governance practice (IODSA, 2009a:84). Gartner (2010:1) found that CIO's who successfully implement pragmatic IT governance are able to deliver greater business value from IT, help the business become more competitive and enable higher user satisfaction.

- **CIO on executive committee and CIO reporting to the CEO and/or COO** are IT governance practices which can be utilised to directly address three IT governance principles of KINGIII and two indirectly. These IT governance practices are also specifically referred to in KINGIII under IT governance principle three (IODSA, 2009a:84). The utilisation of this IT governance practice to effectively implement IT governance is supported by the findings of Luftman et al. (1999:4) who identified that senior executive support for IT is the most important enabler to improve IT and business alignment which is one of the most important IT governance objectives as already discussed above. The effectiveness of these IT governance practices is further supported through research conducted by Ferguson, Green, Vaswani and Wu (2013:89) who confirmed that the involvement of senior management in IT positively influences the level of effective IT governance.

  In an effort to obtain a deeper understanding of dimensions that could help understand top management's knowledge of IT governance, Ali, Green and Robb (2013:137) conducted research to measure top management's knowledge absorptive capacity. Green et al. found that for a company to increase its ability to recognize the value of new external information, to fully understand it and to apply it to gain commercial benefits, top management should focus on four dimensions, including "(1) prior relevant knowledge, (2) an effective communication network, (3) an appropriate communication climate and (4) effective knowledge scanning".

- The objective of the IT governance process **IT governance assurance and self-assessment** is the performance of regular self-assessments or independent assurance activities with regards to the governance of and control over IT (De Haes & Van Grembergen, 2009:449). KINGIII under IT governance principles four and seven requires the board to obtain assurance in respect of IT in certain instances (IODSA, 2009a:85 – 87).

- The IT governance structures **IT strategy committee at level of board of directors** and **IT steering committee** are the ninth and tenth IT governance practices identified in the analysis which can be used to implement IT governance.

  The **IT strategy committee** at the level of the board of directors is an IT governance structure that can be implemented to directly address five of the IT governance principles in KINGIII. Although the Report does not make direct reference to an IT strategy committee, it does refer to an IT steering committee (IODSA, 2009a:83). KINGIII however places the IT steering committee at the board of directors' level with the objective being to support the board with its governance of IT. It therefore appears that what KINGIII refers to as an IT steering committee is, in the context of the De Haes and Van Grembergen (2008:449) list of validated IT governance structures, an IT strategy committee. The IT Governance Institute (ITGI, 2003:57), in its Board Briefing on IT Governance, also makes reference to an IT strategy committee at the level of the board of directors.

  In essence, it is the **responsibility** of the IT strategy committee to provide advice and insight to the board on relevant IT governance topics, to provide direction to management in line with the IT strategy approved by the board and to act as the driver for the board's IT governance practices. The IT strategy committee has the **authority** to advise the board and management on IT strategy, to provide input to the IT strategy and prepare it for approval by the board and to focus on current and future strategic IT matters. The **membership** of the committee is made up of board members and selected specialist non-board members (ITGI, 2003:57).

The **IT steering committee** is situated at the **executive management** level (De Haes & Van Grembergen, 2008:449). De Haes and Van Grembergen (2008:452) found that an IT steering committee is the IT governance practice that is the most effective, when compared to the other 32 IT governance practices, and is relatively easy to implement. This is supported by the finding of research conducted by Ferguson et al. (2013:88) which found that the existence of an effective IT steering committee positively influences the level of effective IT governance.

As explained by the IT Governance Institute (2003:57), the **responsibilities** of the IT steering committee comprise of management responsibilities, which includes the alignment and approval of the enterprise architecture, the acquisition and assignment of appropriate resources, as well as monitoring and communication. The committee has the **authority** to assist executive management with the delivery of the IT strategy, to oversee the day-to-day management of IT projects and service delivery and to focus on implementation. The **membership** of the committee comprises of sponsoring executive management, business executives, the CIO and key advisors that may be required from time to time.

To conclude on this section of the research, the top ten IT governance practices identified in the analysis set out in Table 3, was further analysed in the context of the discussions set out above and the findings of De Haes and Van Grembergen (2008:450) on the perceived effectiveness and ease of implementation of the relevant IT governance practices. The results of this further analysis are presented in Table 4.

Table 4: Perceived effectiveness (PE) and ease of implementation (PEI) of the top ten IT governance practices identified in Table 3

De Haes and Van Grembergen (2008:449) validated list of ITG practices					Count of P	Count of S	Count of K3	SUM of P; S; K3
S, P or M	**#**	**PE**	**PEI**	**Description** of ITG structure, process or relational mechanism				
S	1	4.6	3.4	**IT steering committee (IT investment evaluation / prioritisation at execution / senior management level)**	**3**	**1**	**1**	**5**
S	2	4.5	4.2	**CIO reporting to CEO and/or COO**	**3**	**2**	**1**	**6**
S	3	4.4	3.5	**CIO on executive committee**	**3**	**2**	**1**	**6**
M	4	3.9	2.8	**IT leadership**	**4**	**1**	**1**	**6**
S	5	3.8	3.4	**IT strategy committee at level of board of directors**	**5**	**0**	**0**	**5**
P	6	3.8	2.8	**Strategic information systems planning**	**3**	**3**	**1**	**7**
P	7	3.3	2.4	**IT governance framework COBIT**	5	2	3	10
S	8	3.2	3.4	(IT) audit committee at level of board of directors	2	4	2	8
S	9	3.1	2.2	IT expertise at level of the board of directors	6	0	0	6
P	10	2.8	2.5	IT governance assurance and self-assessment	2	4	0	6

Table 4 was constructed in the same manner as Table 3, except that only the top ten IT governance practices were included in this table. The concepts of perceived effectiveness (PE) and perceived ease of implementation (PEI) was also added to the analysis based on the scores determined by De Haes and Van Grembergen (2008:450) for the top ten IT governance practices. The table was subsequently sorted firstly based on PE and secondly based on PEI. The results of this analysis can be used to determine which of the top ten IT governance principles identified in Table 3 should be selected based on ease of implementation and perceived effectiveness.

3.4 Five key IT decisions that have to be addressed in respect of the management and use of IT

The first IT governance principle of KINGIII requires that the IT governance framework should facilitate and enhance the company's ability to reach its stated objectives by making the most appropriate decisions about incorporating IT into the operations of the business (IODSA, 2009a:82).

Weill and Ross (2004b:8) defined IT governance as "specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT". This definition is in line with the first IT governance principle in KINGIII, which requires the board to ensure that an IT governance charter and policies is established and implemented (IODSA, 2009a:82). The charter and policies should outline the decision making rights and accountability framework for IT governance that will enable the desirable culture in the use of IT within the company.

As part of their research into decision rights, Weill and Ross (2004b:26 – 49) introduced five key IT decisions that every enterprise has to attend to in order to make IT a strategic asset, which includes (1) IT principles, (2) IT architecture, (3) IT infrastructure, (4) business application needs and (5) IT investment and prioritization.

The five key IT decisions introduced by Weill and Ross was mapped to the seven IT governance principles of KINGIII with the results reflected in Table 5. The results of this analysis demonstrates that addressing all five key IT decisions will also address all the IT governance principles of KINGIII.

Table 5: KINGIII IT governance principles mapped to the five key IT decisions

KINGIII ITG PRINCIPLES (IODSA, 2009a)		**Five Key IT Decisions: making IT a strategic asset (Weill & Ross, 2004b:25 - 49)**				
		Decision 1	**Decision 2**	**Decision 3**	**Decision 4**	**Decision 5**
Principle	**Description of principle**	*IT Principles*	*IT Architecture*	*IT Infrastructure*	*Business application needs*	*IT investment and prioritization*
Principle 1	The board should be responsible for ITG	x				
Principle 2	IT should be aligned with the performance and sustainability objectives of the company	x				
Principle 3	The board should delegate to management the responsibility for the implementation of an ITG framework	x	x	x	x	x
Principle 4	The board should monitor and evaluate significant IT investments and expenditure					x
Principle 5	IT should form an integral part of the company's risk management			x		

Principle 6	The board should ensure that information assets are managed effectively			x		
Principle 7	A risk committee and audit committee should assist the board in carrying out its IT responsibilities			x		x

Each of the five key IT decisions will be discussed in more detail below.

3.4.1 Decision 1: IT principles

Weill and Ross (2004b:27) explain that IT principles are a related set of high-level statements about how IT is used in a business. To achieve its objectives, a business defines and articulates its business principles. These business principles in turn are used to define and articulate a set of **IT principles** for the business. The effectiveness of the set of IT principles is dependent on how clear the link is between the IT principles and the business principles from which they have been derived (Weill & Ross, 2004b:28).

The set of IT principles of a business should define the desirable behaviour which is expected from both IT users and IT professionals. According to Weill and Ross (2004b:30), IT principles should clarify at least three expectations for IT in the business, namely:

- The desired operating model of the enterprise.
- How IT will support the desired operating model of the enterprise.
- How IT will be funded.

The IT principles of a business provide the direction for all the IT decisions made by that business. If the IT principles of a business is therefore not clearly defined and articulated, the results of the other IT decisions will be negatively affected (Weill & Ross, 2004b:30).

3.4.2 Decision 2: IT architecture

"The IT architecture of a business is the organizing logic for data, applications and infrastructure, captured in a set of policies, relationships and technical choices, to achieve desired business and technical standardisation and integration" (Weill & Ross, 2004b:30). **The IT architecture decision is important for the effective management and use of IT as it provides a roadmap for the IT infrastructure (decision 3) and application (decision 4) decisions.**

The IT capabilities of a business are shaped through integration and standardisation which in turn is dependent on an organizing logic for data, applications and infrastructure (Weill & Ross, 2004b:30). Process **integration** provides the ability to various business units to view the same data from the perspective of their respective processes. Data standardization is the architectural requirement for process integration. Process **standardisation**, as opposed to process integration, is the disciplined adherence to a consistent way of doing things. It provides predictability and efficiency for the processes being followed.

3.4.3 Decision 3: IT infrastructure

"IT infrastructure is the foundation of planned IT capability (both technical and human) available throughout the business as shared and reliable services and used by multiple applications" (Weill & Ross, 2004b:34 – 35). Weill and Ross propose that the IT infrastructure of a business consists of services in ten clusters, as set out in Table 6.

Table 6: IT infrastructure services in ten clusters

IT infrastructure cluster	Description of IT infrastructure service
Integrated electronic channels	Business partners obtain electronic access to a business via integrated electronic channels. These channels could include a physical outlet, the internet, e-mail, wireless devices, etc. Generally, enterprises try to make their applications channel independent; which means that consistent up to date data is available regardless of the method used by the customer to make contact with the business.
Security and risk	All communications with the business must pass through a security and risk capability. This capability provides security through the use of technologies, policies and disaster planning and recovery.
Communications	Communication services which include workstation networks, intranet and broadband.
Data management	Data management services which include database management, middleware management and data exchange translations.
Infrastructure applications	Enterprise wide infrastructure applications that are used to capture, update and access enterprise data.
IT facilities management	IT infrastructure services which span the IT infrastructure clusters set out above. It includes providing services such as a common systems development environment, large scale processing, etc.
IT management	IT management services which include information systems planning, project management, service level agreements and negotiations with vendors and outsourcers. These services co-ordinate the integrated enterprise infrastructure and manage relationships with business units.
IT architecture and standards	Architecture services which includes monitoring the effectiveness of the business's standards and identifying when those standards are outdated or too costly to support.
IT education and training	IT education and training services which includes training staff in the use of the business's specific technologies and IT systems and general management training on how to create business value from IT.

IT research and development	IT research and development services which includes processes to identify new ways of using IT to create business value and to assess how new technologies can be used in the business.

Source: Weill and Ross (2004b:38)

Weill and Ross (2004b:39) found that enterprises that manage IT infrastructure as an asset and invests in IT infrastructure on a consistent and annual basis, typically perform better than enterprises with an approach of investing in IT infrastructure in a reactive manner.

3.4.4 Decision 4: Business application needs

The identification of business needs for IT applications has two objectives, namely creativity and discipline. *Creativity* involves the identification of new and more effective ways of delivering value to customers using IT. *Discipline* relates to architectural integrity, which means that new applications should leverage and build on the enterprise's architecture rather than undermine the established architecture principles. These objectives of creativity and discipline are often conflicting (Weill & Ross, 2004b:40).

3.4.5 Decision 5: IT investment and prioritization

According to Weill and Ross (2004b:45), IT investment decisions address three areas, namely (1) how much funds to spend on IT, (2) what the designated funds should be spent on and (3) how the needs of different parts of the business should be reconciled when deciding how much funds to spend and what to spend it on.

3.4.6 IT governance structures that can be used to provide input into or take each of the five key IT decisions

In section 3.3, IT governance structures, processes and relational mechanisms were discussed in some detail. In order to determine which of the IT governance **structures**, as identified by De Haes and Van Grembergen (2008:449), could be

used to (1) **provide input** into making each of the five key IT decisions and (2) to **take** each of the five key IT decisions, the IT governance **structures** were mapped to the five key IT decisions identified by Weill and Ross (2004b:25 – 49). Refer to Table 7.

Table 7: Five key IT decisions and IT governance structures

De Haes and Van Grembergen Information Technology Governance (ITG) structures (De Haes & Van Grembergen, 2008:449)			**Five Key IT Decisions: making IT a strategic asset (Weill & Ross, 2004b:25 - 49)**				
			Decision 1	**Decision 2**	**Decision 3**	**Decision 4**	**Decision 5**
Structure (S)	**Description** of ITG structure, process or relational mechanism	**Definition** of ITG structure, process or relational mechanism	*IT Principles*	*IT Architecture*	*IT Infrastructure*	*Business application needs*	*IT investment and prioritization*
S	IT strategy committee at level of board of directors	Committee at level of board of directors to ensure IT is regular agenda item and reporting issue for the board of directors	Decision	Decision	Input	Input	Decision
S	IT expertise at level of the board of directors	Members of the board of directors have expertise and experience regarding the value and risk of IT	Input	Input	Input	Input	Input
S	(IT) audit committee at level of board of directors	Independent committee at level of board of directors overviewing (IT) assurance activities	Input	Input	Decision (specifically relating to risk)	Input	Input
S	CIO on executive committee	CIO is full member of the executive committee	Input	Input	Input	Input	Input
S	CIO reporting to CEO and/or COO	CIO has direct reporting line to the CEO and/or COO	Input	Decision / input	Decision / input	Input	Input

S	IT steering committee (IT investment evaluation / prioritisation at execution / senior management level)	Steering committee at executive or senior management level responsible for determining business priorities in IT investments	Input	Input	Decision	Decision	Decision
S	ITG function / officer	Function in the organisation responsible for promoting, driving and managing IT governance processes	Input	Input	Input	Input	Input
S	Security / compliance / risk officer	Function responsible for security, compliance and/or risk, which possibly impacts IT			Input (specifically relating to security)		
S	IT project steering committee	Steering committee composed of business and IT people focusing on prioritising and managing IT projects			Decision	Decision	Decision / input
S	IT security steering committee	Steering committee composed of business and IT people focusing on IT related risks and security issues			Decision (specifically relating to security)		
S	Architecture steering committee	Committee composed of business and IT people providing architecture guidelines and advise on their applications		Decision	Input	Input	
S	Integration of governance / alignment tasks in roles & responsibilities	Documented roles & responsibilities include governance / alignment tasks for business and IT people	Input	Input	Input	Input	Input

In Table 7, the structures that could be used to provide input into the taking of each of the five key IT decisions was mapped to the relevant decision with the key 'Input'. Similarly, the structures that could be used to take each of the five key IT decisions were mapped to the relevant decisions with the key 'Decision'. This analysis can be used as a reference when allocating decision rights and accountability as required by KINGIII (IODSA, 2009a:82).

3.5 Acquire and maintain relevant competences required to govern and / or manage IT

Cragg, Caldeira and Ward (2011:353) used resource-based theory and evidence that they gathered from empirical studies to evolve a framework of information system (IS) competencies in small and medium-sized entities (SME's). The framework is a comprehensive set of IT competences that can be used in practice by SME's.

Cragg et al. (2011:354) used the following definitions in their study. *Resources* were defined to include knowledge, physical and financial assets. *Capabilities* were defined as an organizations capacity to deploy a combination of resources through organizational processes to achieve desired goals. *Competences* were defined as the ability to develop, manage and deploy resources in support of capabilities.

Cragg et al. (2011:357) developed the framework of organizational IS competence's in SME's from a number of sources, through a process of repeated comparative assessments through which revised versions were created after considering each new source and by taking empirical data of 22 case studies into account. The resultant framework consists of 22 competencies classified into six macro competencies, as set out in Table 8.

Table 8: Cragg, Caldeira and Ward framework of organizational IS competences in SME's

Macro competence (MC)	Competence (C)
MC1: Business and information system (IS) strategic thinking	C1: IS innovation
	C2: Business case and investment criteria
	C3: Including IS in business strategy
	C4: Information governance
MC2: Define IS contribution	C5: IS alignment
	C6: Business process management
	C7: Define IS requirements
	C8: Accessing IS knowledge
MC3: Define the IS strategy	C9: Software sourcing strategies
	C10: IS acquisition processes
	C11: Technology infrastructure requirements
MC4: Exploitation	C12: Benefits management
	C13: Managing change
	C14: Project management
	C15: Inter-organizational collaboration
MC5: Deliver solutions	C16: Applications development
	C17: Implementation and integration
	C18: Apply and use technology
	C19: Business continuity and security
MC6: Supply	C20: Manage IS supplier relationships
	C21: Information asset management and maintenance
	C22: Staff development

Source: Cragg et al. (2011:357)

The framework of organizational IS competences was mapped to the IT governance principles of KINGIII to determine to what extent the competences identified in the Cragg et al. framework can be utilised to address the KINGIII IT governance principles. The detailed results of this analysis is included as Appendix B: Cragg et al. (2011:357) framework of organizational IS competences in SME's mapped to the IT governance principles of KINGIII (IODSA, 2009a). In summary, the analysis indicates that all the competences identified by Cragg et al. can be utilised to address the IT governance principles of KINGIII.

The framework of organizational IS competences was also mapped to the five key IT decisions introduced by Weill and Ross (2004b:25 – 49) to indicate which of the competences are related to which of the five key IT decisions. This analysis is included in Appendix C: Cragg et al. (2011:357) framework of organizational IS competences in SME's mapped to the Five Key IT Decisions of Weill and Ross (2004b:25 – 49).

Each of the macro competences as identified by Cragg et al. will be briefly discussed below.

3.5.1 Macro competence 1: Business and IS strategic thinking

This set of four competences relates to an enterprise's ability to identify and evaluate the need for IT in providing the enterprise with opportunities to improve its business strategy and to manage IT activities more effectively. This includes designing an appropriate IT organization and defining roles, responsibilities and policies (Cragg et al., 2011:356). This competence is strongly related to the KINGIII IT governance principles one, two, three and four. This can also be seen from the results of the analysis included in Appendix B.

3.5.2 Macro competence 2: define the IS contribution

This set of four competences involves translating the IT strategy into investments in IT that meet information needs and improvements in business performance. A key

focus is to synchronise (or align) the IT investments with the enterprise's business priorities (Cragg et al., 2011:358). This competence is strongly related to IT governance principle three as contained in KINGIII, but can also be linked to IT governance principles one, two, four, five and six.

3.5.3 Macro competence 3: define the IS strategy

This is a set of three competences which are focussed on (1) defining the information and application architectures, (2) the IT infrastructure and (3) IT resources which are needed to enable the enterprise to successfully acquire and/or implement its resources (Cragg et al., 2009:358). These competences are related to the KINGIII IT governance principles two, three and four.

3.5.4 Macro competence 4: exploitation

To achieve maximum advantages from IT, it is important to have effective IT use processes. This set of four competences therefore relate to the enterprise's ability to increase the benefits from the effective use of investments in information and applications (Cragg et al., 2011:359). This competence mainly relates to the KINGIII IT governance principle three.

3.5.5 Macro competence 5: deliver solutions

Enterprises have to be able to convert IT requirements into working IT assets that perform according to specification and which can be integrated effectively with other business systems and processes (Cragg et al., 2011:359). This set of four competences also mainly relate to the KINGIII IT governance principle three.

3.5.6 Macro competence 6: supply

These three competences are of an operational nature which enables an enterprise to create and maintain its technology resources and applications through the

effective management of the IT supply chain and external and internal IT resources (Cragg et al., 2011:360). This competence mainly relates to IT governance principles two, three and four as set out in KINGIII.

3.6 Conclusion of Chapter 3

The purpose of this chapter was to identify and discuss ***how*** the principles of IT governance can be implemented in practice. To address this objective, the following concepts were analysed and discussed.

Firstly, the concept of an access path was proposed as a method that can be utilised to analyse and document the IT assets of an enterprise in order to develop an understanding of the IT environment that has to be governed and managed.

Secondly, structures, processes and relational mechanisms which can be utilised to implement an IT governance framework was investigated, analysed and discussed. The top ten IT governance practices that can be implemented to apply the IT governance principles of KINGIII was identified and analysed further to determine which of the top ten IT governance practices are perceived to be the most effective and which the simplest to implement.

Thirdly, the five key IT decisions that an organization has to address was discussed and analysed to determine to what extent addressing these IT decisions will assist the board and management to implement effective IT governance. The IT governance structures was also analysed in the context of the five key IT decisions to determine which of the structures can be used to provide input into the decision making process and which can be used to take the relevant decisions.

Lastly, a framework of IS competences in SME's was analysed in the context of the KINGIII IT governance principles to determine to what extent the acquisition and maintenance of each competence can assist the organization to successfully apply the KINGIII IT governance principles. The IS competence framework was also analysed in the context of the five key IT decisions to determine to what extent the IS

competence can assist the organization in addressing each of the five key IT decisions.

Chapter four will build on the discussions and findings of chapters 2 and 3 to compile the practical, step by step approach which can be used by those persons charged with the governance of medium sized enterprises in South Africa, to enable them to successfully bridge the IT gap.

4. Chapter 4: Compilation of the step by step approach to implement IT governance as required by KINGIII

4.1 Introduction to Chapter 4

The purpose of this chapter is to compile the step by step approach that can be followed by those persons charged with the governance of medium sized enterprises in South Africa, to enable them to successfully bridge the IT gap. The compilation of the approach is based on the discussions and findings set out in chapters 2 and 3.

This chapter will also build on the analyses performed in chapters 2 and 3 to compile proposed resolutions to be adopted by the board and documents to be used by management in each step of the approach. In certain instance the relevant documents can be presented by management to the board for their consideration and approval.

4.2 Compilation of the step by step approach

4.2.1 Step 1: Accept responsibility for the governance of IT

The first IT governance principle of KINGIII requires the board of a company to take responsibility for the governance of IT. The other six IT governance principles of KINGIII are all dependent on the application by the board of principle one. As the first step, the board should therefore accept responsibility for the governance of IT in the organization.

4.2.2 Step 2: Obtain an understanding of the KINGIII principles of IT governance

Once the board of a company has resolved to implement the IT governance principles of KINGIII, the next step would be for them to obtain an in-depth

understanding of the seven IT governance principles of KINGIII, as well as the 24 recommended practices and the detailed narrative discussions contained in the Report. To assist the board with this process, chapter 2 of this research discusses each of the seven IT governance principles of KINGIII in the context of the 24 recommended practices, detailed narrative discussions and other relevant literature on IT governance.

4.2.3 Step 3: Identify and analyse the IT assets of the organisation

KINGIII requires the board to take responsibility for the governance of IT. This includes all the IT assets of the business. The first IT governance principle of KINGIII states that the board should understand IT, including the benefits, risks and constraints relating to IT. As discussed in chapter 3, Weill and Ross (2004b:6) pointed out that IT assets are key assets to any organization in the same manner as human assets, financial assets, physical assets, intellectual property and relationship assets. Accordingly, in chapter 3 it was proposed that the concept of **access paths**, as formulated by Boshoff (1990:24), can be utilised to identify and analyse the IT assets of the organization in order for the board and management to develop an understanding of the IT environment of the organization, including the related benefits, risks and constraints.

4.2.4 Step 4: Identify and approve appropriate structures, processes and relational mechanisms for the implementation of IT governance

Through the analysis of the first IT governance principle of KINGIII, it was identified that the board should adopt an IT governance framework which includes relevant **structures, processes and mechanisms** to enable IT to deliver the required value to the company. The board should, within the specific context of the company being governed, approve appropriate IT governance practices (which includes structures, processes and relational mechanisms) to successfully implement IT governance in the organization. Available structures, processes and relational mechanisms were discussed and analysed in chapter 3 (refer to section 3.3 on page 33) in order to assist the board and management to determine which of the structures, processes

and relational mechanisms would be appropriate for the implementation of the IT governance principles of KINGIII in their company.

4.2.5 Step 5: Implement the approved IT governance practices and ensure that the five key IT decisions are addressed

Once the board has adopted an IT governance framework which includes relevant structures, processes and relational mechanisms in terms of step 4 of this approach, the next step would be to implement the identified and adopted IT governance practices. In terms of the first IT governance principle of KINGIII, the IT governance framework should enhance the company's ability to achieve its objectives by taking the most appropriate **decisions** about how to incorporate IT into the operations of the business. To address this requirement, **five key decisions** in respect of IT was identified and discussed in chapter 3. The five key decisions include (1) IT principles, (2) IT architecture, (3) IT infrastructure, (4) business application needs and (5) IT investment and prioritization. As part of the design of the IT governance for the organization the board should also assign the decision making responsibilities in respect of each of these five key decisions to relevant IT governance structures. Each of the five key decisions were therefore analysed in the context of the IT governance structures identified to assist the board with the allocation of these decision rights.

4.2.6 Step 6: Acquire and maintain relevant competences which are required to implement the selected IT governance practices

Lastly, in terms of the discussion of IT governance principle four in chapter 2, it was identified that a company should acquire and use appropriate technology, processes and people to support its IT governance requirements. A framework of information systems (IS) competencies was accordingly identified and discussed in chapter 3 in the context of the IT governance principles of KINGIII and the five key IT decisions which have to be addressed. The board and management should ensure that the organization has the relevant competencies in place to enable them to successfully address the IT governance principles of KINGIII.

4.3 Practical implementation of the step by step approach

The step by step approach to implement IT governance as required by KINGIII was formulated and discussed in section 4.2 above. The approach contains six steps that should be followed to successfully implement IT governance. Whereas section 4.2 focused on the compilation of the step by step approach, this section of the research will focus on practical steps that the board and/or management can take to follow the step by step approach as formulated above.

To assist the reader with linking together the various parts of this research and to assist the reader with the practical implementation of the approach, a summary of the compiled step by step approach has been included in Table 9.

Table 9: Summary of the compiled step by step approach

Step in approach	Description of step	KINGIII IT governance principle/(s) addressed by step	Related chapters and sections in this research	Proposed wording and/or formats for documents that can be used for each step
Step 1	Accept responsibility for the governance of IT	Principle 1	Chapter 2, section 2.3 and Chapter 4, sections 4.2.1 and 4.3.1.	Proposed wording for a board resolution. Refer to section 4.3.1.
Step 2	Obtain an understanding of the KINGIII principles of IT governance	Principles 1 to 7	Chapter 2 and Chapter 4, sections 4.2.2 and 4.3.2.	Proposed checklist. Refer to Table 10.
Step 3	Identify and analyse the IT assets of the organisation	Principle 1	Chapter 3, section 3.2 and Chapter 4, sections 4.2.3 and 4.3.3.	Proposed format for the documentation and analysis of the IT environment. Refer to Table 11.
Step 4	Identify and approve appropriate structures, processes and relational mechanisms for the implementation of IT	Principles 1 to 7	Chapter 3, section 3.3 and Chapter 4, sections 4.2.4 and 4.3.4.	Reference list for the identification of relevant IT governance practices. Refer to

	governance			Table 12.
Step 5	Implement the approved IT governance practices and ensure that the five key IT decisions are addressed	Principles 1 to 7	Chapter 3, section 3.4 and Chapter 4, sections 4.2.5 and 4.3.5.	Proposed format for documenting which IT governance structures should be used for input and for taking the key IT decisions. Refer to Table 13.
Step 6	Acquire and maintain relevant competences which are required to implement the selected IT governance practices	Principles 1 to 7	Chapter 3, section 3.5 and Chapter 4, sections 4.2.6 and 4.3.6.	Proposed format for the identification and analysis of competences required by the company. Refer to Table 14.

4.3.1 Step 1: Accept responsibility for the governance of IT

In order for the board of a company to accept responsibility for the governance of IT as required by KINGIII, it is proposed that the following resolution be taken by the board and recorded in the minutes of the meeting of the directors where the resolution is adopted:

"Resolution of the board of directors

The board is committed to the application of the principles of IT governance as set out in KINGIII. The first principle of IT governance contained in KINGIII requires that the board should be responsible for the governance of IT.

Therefore,

It is **resolved**, that the board accepts responsibility for the governance of IT and that IT governance will be placed on the board agenda as a permanent item to be discussed at all board meetings.

It is **also resolved** that the board delegate to management the responsibility to document and analyse the company's IT environment by utilising the concept of **access paths** and presenting the completed analysis to the board for consideration and approval.

It is **further resolved** that the board delegate to management the responsibility to make recommendations to the board, for the board's consideration and approval, in respect of the following:

- Relevant **structures, processes and mechanisms** which should be adopted by the company to apply the IT governance principles of KINGIII.
- Relevant **structures** which should be used to provide input to and take the **five key IT decisions**.
- Relevant **competences** which should be acquired and/or maintained by the company in order to implement the IT governance practices proposed by management for the application of the IT governance principles of KINGIII.**"**

4.3.2 Step 2: Obtain an understanding of the KINGIII principles of IT governance

The board and/or management of a company should obtain an in-depth understanding of the seven IT governance principles, and the 24 recommended practices, set out in KINGIII. To assist the board and/or management to ensure that they obtain an understanding of **all** the IT governance principles and recommended practices in KINGIII, the checklist set out in Table 10 can be used. The checklist has been derived from Table 1 in chapter 2.

Table 10: IT governance principles and recommended practices checklist

Principle (P)	Recommended practice/(s) (RP)	Do you understand the **P** and **RP** set out in columns 1 and 2? Circle **YES** or **NO****
P1: the board should be responsible for IT governance	**RP1:** the board should assume responsibility for the governance of IT and place it on the board agenda.	**YES** or **NO**
	RP2: the board should ensure that an IT charter and policies are established and implemented.	**YES** or **NO**
	RP3: the board should ensure promotion of an ethical culture and awareness and a common IT language.	**YES** or **NO**
	RP4: the board should ensure that an IT internal control framework is adopted and implemented.	**YES** or **NO**
	RP5: the board should receive assurance on the effectiveness of the IT internal controls.	**YES** or **NO**
P2: IT should be aligned with the performance and sustainability objectives of the company	**RP6:** the board should ensure that the IT strategy is integrated with the company's strategic and business processes.	**YES** or **NO**
	RP7: 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.	**YES** or **NO**
P3: the board should delegate to management the responsibility for the implementation of an IT governance framework	**RP8:** management should be responsible for the implementation of the structures, processes and mechanisms for the IT governance framework.	**YES** or **NO**
	RP9: the board may appoint an IT steering committee of similar function to assist with its IT governance.	**YES** or **NO**
	RP10: the CEO should appoint a Chief Information Officer ('CIO') responsible for the management of IT.	**YES** or **NO**
	RP11: the CIO should be a 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.	**YES** or **NO**
P4: the board should monitor and evaluate significant IT investments and expenditure	**RP12:** the board should oversee the value delivery of IT and monitor the return on investment from significant IT projects.	**YES** or **NO**
	RP13: the board should ensure that intellectual property contained in information systems is protected.	**YES** or **NO**
	RP14: the board should obtain independent assurance on the IT governance and controls supporting outsourced IT services.	**YES** or **NO**
P5: IT should form an integral part of the company's risk	**RP15:** management should regularly demonstrate to the board that the company has adequate business resilience arrangements in place for disaster recovery.	**YES** or **NO**

management	**RP16:** the board should ensure that the company complies with IT laws and that IT related rules, codes and standards are considered.	**YES** or **NO**
P6: the board should ensure that information assets are managed effectively	**RP17:** the board should ensure that there are systems in place for the management of information which should include information security, information management and information privacy.	**YES** or **NO**
	RP18: the board should ensure that all personal information is treated by the company as an important business asset and is identified.	**YES** or **NO**
	RP19: the board should ensure that an Information Security Management system is developed and implemented.	**YES** or **NO**
	RP20: the board should approve the information security strategy and delegate and empower management to implement the strategy.	**YES** or **NO**
P7: a risk committee and audit committee should assist the board in carrying out its IT responsibilities	**RP21:** the risk committee should ensure that IT risks are adequately addressed.	**YES** or **NO**
	RP22: the risk committee should obtain appropriate assurance that controls are in place and effective in addressing IT risks.	**YES** or **NO**
	RP23: the audit committee should consider IT as it relates to financial reporting and the going concern of the company.	**YES** or **NO**
	RP24: the audit committee should also consider the use of technology to improve audit coverage and efficiency.	**YES** or **NO**

**in instances where NO is selected, the person completing the checklist should revisit chapter 2 of this research and, if necessary, chapter 5 and section 5 of the KINGIII Report and Code respectively.

4.3.3 Step 3: Identify and analyse the IT assets of the organisation

As discussed in section 3.2 of chapter 3, the concept of **access paths** can be used to analyse and obtain an understanding of the IT environment of the company. Figure 1 on page 33 illustrates the concept of an access path.

The tabular format set out in Table 11 can be utilised to document and analyse the IT environment of a company:

Table 11: Format for the documentation and analysis of the IT environment

Description of technology component (TC)	Benefits relating to TC	Risks relating to TC	Constraints relating to TC
TC 1:			
TC 2:			
TC 3:			
TC 4:			
TC n:			
Example:			
TC 1: Microsoft Windows	*Microsoft Windows is a generally used and well supported operating system. People are in most instances familiar with and able to use the software without further training.*	*The operating system has to be kept updated at all times to ensure that weaknesses identified by the developer of the software are remedied before it has a negative impact on the company.*	*Windows is a packaged operating system and can only be customised to the extent allowed by the configuration choices of the software. Further customisation will not be possible.*

Column 1 sets out all the different components in the access path; with TC 1 being the first technology component and TC n the last component in the access path being documented and analysed. In columns 2 to 4, the person analysing each of the components in the access path should document the benefits, risks and constraints relating to the relevant technology component. An example has been included to demonstrate how the document should be completed.

As the analysis of the different access paths (and as a result the IT environment) will inevitably require some technical IT knowledge, the documentation and analysis of the access paths of a company will require the inputs of both business management and IT management in order to arrive at a complete and accurate result.

Management can present the completed document to the board for their information and to assist them in developing an understanding of the IT environment of the company.

4.3.4 Step 4: Identify and approve appropriate structures, processes and relational mechanisms for the implementation of IT governance

The board should, within the specific context of the company being governed, approve appropriate IT governance practices to successfully implement IT governance in the organization.

The IT governance practices discussed in section 3.3 of chapter 3 and set out in Table 3 can be used by management to identify relevant structures, processes and relational mechanisms which should be recommended for approval to the board and implementation by management. Refer to Table 12 for the proposed format to be used for the identification of relevant IT governance practices. Table 12 has been derived from Table 3 on page 35.

Table 12: Identification of relevant IT governance structures, processes and relational mechanisms

De Haes and Van Grembergen (2008:449) validated list of ITG practices				
S, P or M	#	**Description** of ITG structure, process or relational mechanism	Is the **ITG structure, process or relational mechanism** relevant to the organization and should the adoption thereof be proposed to the board of directors? Circle **YES** or **NO**.	If **YES** was selected, please motivate why the ITG structure, process or relational mechanism should be adopted by the company. If **NO** was selected, please explain why the ITG structure, process or relational mechanism is not relevant.
P	1	IT governance framework COBIT	**YES** or **NO**	
S	2	(IT) audit committee at level of board of directors	**YES** or **NO**	
P	3	Strategic information systems planning	**YES** or **NO**	
S	4	IT expertise at level of the board of directors	**YES** or **NO**	
M	5	IT leadership	**YES** or **NO**	
S	6	CIO on executive committee	**YES** or **NO**	
S	7	CIO reporting to CEO and/or COO	**YES** or **NO**	
P	8	IT governance assurance and self-assessment	**YES** or **NO**	
S	9	IT strategy committee at level of board of directors	**YES** or **NO**	
S	10	IT steering committee (IT investment evaluation / prioritisation at execution / senior management level)	**YES** or **NO**	
S	11	ITG function / officer	**YES** or **NO**	
S	12	Integration of governance / alignment tasks in roles & responsibilities	**YES** or **NO**	
P	13	Portfolio management (incl. business cases, information economics, ROI, payback)	**YES** or **NO**	
P	14	Service level agreements	**YES** or **NO**	
M	15	ITG awareness campaigns	**YES** or **NO**	
P	16	IT budget control and reporting	**YES** or **NO**	

P	17	IT performance measurement (e.g. IT balanced scorecard)	**YES** or **NO**	
S	18	IT security steering committee	**YES** or **NO**	
P	19	Project governance / management methodologies	**YES** or **NO**	
S	20	IT project steering committee	**YES** or **NO**	
S	21	Architecture steering committee	**YES** or **NO**	
P	22	COSO / ERM	**YES** or **NO**	
M	23	Corporate internal communication addressing IT on a regular basis	**YES** or **NO**	
M	24	Information meetings between business and IT executives / senior management	**YES** or **NO**	
M	25	Executive / senior management giving the good example	**YES** or **NO**	
M	26	Job-rotation	**YES** or **NO**	
M	27	Co-location	**YES** or **NO**	
M	28	Cross-training	**YES** or **NO**	
M	29	Knowledge management (on ITG)	**YES** or **NO**	
M	30	Business / IT account management	**YES** or **NO**	
S	31	Security / compliance / risk officer	**YES** or **NO**	
P	32	Charge back arrangements – total cost of ownership (e.g. activity based costing)	**YES** or **NO**	
P	33	Benefits management and reporting	**YES** or **NO**	

Table 12 should be completed by management and the completed document should be presented to the board for their consideration and approval; after which the approved IT governance structures, processes and relational mechanisms can be implemented by management.

4.3.5 Step 5: Implement the approved IT governance practices and ensure that the five key IT decisions are addressed

The five key IT decisions, as discussed in section 3.4 of chapter 3, should be addressed by management. Management should identify the relevant IT governance **structures** that should be used by the company to (1) provide input to and (2) take the relevant IT decision.

An adaptation of Table 7, discussed in section 3.4.6 of chapter 3, can be used by management to prepare a document setting out which of the approved IT governance structures should be used to (1) provide input to and (2) take the relevant key IT decisions. It is proposed that the format set out in Table 13, can be

used to document which structures should be used to provide input and which should be used to take the key IT decisions. The structures available to choose from in Table 13 will be dependent on the structures proposed to and approved by the board in terms of step 4.

Table 13: Identification of the IT governance structures that should provide input to and take the five key IT decisions

De Haes and Van Grembergen Information Technology Governance (ITG) structures (De Haes & Van Grembergen, 2008:449)			**Five Key IT Decisions: making IT a strategic asset (Weill & Ross, 2004b:25 - 49)**				
			Decision 1	**Decision 2**	**Decision 3**	**Decision 4**	**Decision 5**
Structure (S)	**Description** of ITG structure, process or relational mechanism	**Definition** of ITG structure, process or relational mechanism	*IT Principles*	*IT Architecture*	*IT Infrastructure*	*Business application needs*	*IT investment and prioritization*
S	IT strategy committee at level of board of directors	Committee at level of board of directors to ensure IT is regular agenda item and reporting issue for the board of directors	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****
S	IT expertise at level of the board of directors	Members of the board of directors have expertise and experience regarding the value and risk of IT	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****
S	(IT) audit committee at level of board of directors	Independent committee at level of board of directors overviewing (IT) assurance activities	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****
S	CIO on executive committee	CIO is full member of the executive committee	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****
S	CIO reporting to CEO and/or COO	CIO has direct reporting line to the CEO and/or COO	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****

S	IT steering committee (IT investment evaluation / prioritisation at execution / senior management level)	Steering committee at executive or senior management level responsible for determining business priorities in IT investments	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****
S	ITG function / officer	Function in the organisation responsible for promoting, driving and managing IT governance processes	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****
S	Security / compliance / risk officer	Function responsible for security, compliance and/or risk, which possibly impacts IT	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****
S	IT project steering committee	Steering committee composed of business and IT people focusing on prioritising and managing IT projects	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****
S	IT security steering committee	Steering committee composed of business and IT people focusing on IT related risks and security issues	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****
S	Architecture steering committee	Committee composed of business and IT people providing architecture guidelines and advise on their applications	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****
S	Integration of governance / alignment tasks in roles & responsibilities	Documented roles & responsibilities include governance / alignment tasks for business and IT people	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****	**Decision** or **Input****

**circle the relevant choice.

The completed document should be presented to the board for their consideration and approval. Once approved, the different structures can be mandated to fulfil their functions as directed by the board.

4.3.6 Step 6: Acquire and maintain relevant competences which are required to implement the selected IT governance practices

A company should acquire and use appropriate technology, processes and people to support its IT governance requirements.

The framework of information systems (IS) competencies set out in Table 8 and discussed in section 3.5 of chapter 3 can be used to prepare an analysis of the competences required to implement IT governance within the organization. The proposed format is set out in Table 14.

Table 14: Analysis of IS competences required by the organization to implement the IT governance principles of KINGIII

Macro competence (MC)	Competence (C)	Is the MC or C relevant to the organization?	If the answer in column 3 is YES, indicate whether or not the organization has this competence in place?	If the answer in column 4 is NO, explain how the competence will be acquired	If the answer in column 4 is NO, indicate WHO will be required to acquire the competence
MC1: Business and information system (IS) strategic thinking	C1: IS innovation	**YES** or **NO**	**YES** or **NO**		
	C2: Business case and investment criteria	**YES** or **NO**	**YES** or **NO**		
	C3: Including IS in business strategy	**YES** or **NO**	**YES** or **NO**		

	C4: Information governance	**YES** or **NO**	**YES** or **NO**
MC2: Define IS contribution	C5: IS alignment	**YES** or **NO**	**YES** or **NO**
	C6: Business process management	**YES** or **NO**	**YES** or **NO**
	C7: Define IS requirements	**YES** or **NO**	**YES** or **NO**
	C8: Accessing IS knowledge	**YES** or **NO**	**YES** or **NO**
MC3: Define the IS strategy	C9: Software sourcing strategies	**YES** or **NO**	**YES** or **NO**
	C10: IS acquisition processes	**YES** or **NO**	**YES** or **NO**
	C11: Technology infrastructure requirements	**YES** or **NO**	**YES** or **NO**
MC4: Exploitation	C12: Benefits management	**YES** or **NO**	**YES** or **NO**
	C13: Managing change	**YES** or **NO**	**YES** or **NO**
	C14: Project management	**YES** or **NO**	**YES** or **NO**
	C15: Inter-organizational collaboration	**YES** or **NO**	**YES** or **NO**
MC5: Deliver solutions	C16: Applications development	**YES** or **NO**	**YES** or **NO**
	C17: Implementation and integration	**YES** or **NO**	**YES** or **NO**
	C18: Apply and use technology	**YES** or **NO**	**YES** or **NO**
	C19: Business continuity and security	**YES** or **NO**	**YES** or **NO**

MC6: Supply	C20: Manage IS supplier relationships	**YES** or **NO**	**YES** or **NO**
	C21: Information asset management and maintenance	**YES** or **NO**	**YES** or **NO**
	C22: Staff development	**YES** or **NO**	**YES** or **NO**

The completed document should assist management, and the board, to understand the extent of the IS competences of the organization, to identify competences that are required but which the organization does not have in place and to formulate an action plan to acquire the relevant competences which have been identified.

4.4 Conclusion of Chapter 4

The step by step approach that can be followed by those persons charged with the governance of medium sized enterprises in South Africa, to successfully bridge the IT gap was compiled in this chapter. The approach was compiled in the context of the discussions and findings of this research as set out in chapters 2 and 3.

Section 4.2 sets out each of the steps in the approach. Each of the six steps is explained in the context of the discussions and findings of chapters 2 and 3. Section 4.2 also sets out a summary of the approach; please refer to Table 9.

In section 4.3, guidance is provided to the reader to assist with the practical implementation of the step by step approach. The guidance includes proposed wording for resolutions to be adopted by the board of directors as well as proposed formats for documents which can be used in each step of the compiled approach.

5. Chapter 5: Conclusion

5.1 Summary

KINGIII recommends that all entities should apply the governance principles and recommended practices set out in the Code and explained in the Report, and by doing so, achieve good governance (IODSA, 2009a:17). The Code sets out seven IT governance principles and 24 recommended practices that the board and / or management of a company should follow to address the seven IT governance principles.

Governance is focussed on creating value for stakeholders of an enterprise by the realisation of benefits through the optimal utilisation of resources at an acceptable level of risk.

It is important that the board of a company should take responsibility for the governance of IT, not only to fulfil their duties as directors, but also to ensure that the objectives underlying the overall objective of creating value for stakeholders will be achieved. These underlying objectives include (1) benefits realisation, (2) risk optimisation and (3) resource optimisation (ISACA, 2012:17).

The board and business management and staff may not understand IT and the IT management and staff may not understand the principles of governance and the business as a whole. This lack of understanding results in a gap between the business and IT which is referred to as the IT gap. In order for the board and management to effectively utilise IT to achieve the objective of value creation, the IT gap has to be bridged successfully.

The objective of this research was to **compile** a **practical**, **step by step** approach that can be used by those persons charged with the **governance and / or management** of **medium sized enterprises in South Africa**, to **enable** them to successfully **bridge the IT gap.**

To achieve this objective the seven IT governance principles of KINGIII was analysed and discussed in chapter 2. The concepts of (1) governance, (2) information, (3) information technology, (4) principles, (5) practices and (6) policies were defined and the following concepts relating to IT governance identified:

- IT governance structures, processes and mechanisms.
- Five key IT decisions that have to be addressed by the board and management.
- Appropriate technology, processes and people to support the business and its IT governance requirements.

In the context of the findings of chapter 2, chapter 3 explained the concept of access paths and proposed its use for the documentation and analysis of the IT environment of an organization. The IT governance concepts set out above, as identified in chapter 2, were discussed and analysed in the context of relevant literature. From the analysis performed, structures, processes and mechanisms were identified which can be approved by the board and implemented by management to apply the seven IT governance principles of KINGIII. The five key IT decisions that have to be addressed by the board and management were discussed and aligned with IT governance structures that can be utilised to provide input to and / or take the relevant decisions. Lastly, competences that can be utilised to address the IT governance principles of KINGIII and the five key IT decisions were discussed and analysed.

Chapter 4 concluded by setting out the proposed step by step approach for the implementation of IT governance, based on the findings contained in chapters 2 and 3.

5.2 Final conclusion

In conclusion, it is proposed that by following the approach compiled through this research, and summarised in Table 9, the board and / or management of a company should be able to effectively apply the IT governance principles of KINGIII, and by doing so, successfully bridge the IT gap.

5.3 Future research

The step by step approach has been compiled based on an analysis of the IT governance principles of KINGIII, as well as other relevant literature on IT governance, and has not been tested in practice. As a result, there is an opportunity for future research to follow the approach in practice to determine to what extent the approach assists those charged with the governance of organization's to effectively apply the IT governance principles of KINGIII and to successfully bridge the IT gap.

References

Ali, S., Green, P., Robb, A. 2013. Measuring Top Management's IT Governance knowledge absorptive capacity. Journal of Information Systems, 27(1):137 - 155.

Boshoff, W.H. 1990. A path context model for computer security phenomena in potentially non-secure environments. Unpublished doctoral dissertation. Johannesburg: Rand Afrikaans University.

Byrd, T.A., Lewis, B.R., Bryan, R.W. 2006. The leveraging influence of strategic alignment on IT investment: An empirical examination. Information & Management, 43:308 - 321.

Chen, R-S., Sun, C-M., Helms, M.H., Jih, W-J. 2008. Aligning information technology and business strategy with a dynamic capabilities perspective: A longitudinal study of a Taiwanese Semiconductor Company. International Journal of Information Management, 28:366 - 378.

Collins. 2006. Collins Dictionary of Sociology [Online]. Available at: http://www.credoreference.com.ez.sun.ac.za/entry/collinssoc/information technology it [26 September 2013].

Cragg, P., King, M., Hussin, H. 2002. IT alignment and firm performance in small manufacturing firms. Journal of Strategic Information Systems, 11:109 - 132.

Cragg, P., Caldeira, M. & Ward, J. 2011. Organisational information systems competences in small and medium-sized enterprises. Information & Management, 48:353 - 363.

De Haes, S. & Van Grembergen, W. 2009. An exploratory study into IT Governance implementations and its impact on Business/IT alignment. Information Systems Management, 26(2):123 - 137.

De Haes, S. & Van Grembergen, W. 2008. An Exploratory Study into the Design of an IT Governance Minimum Baseline through Delphi Research. Communications of the Association of Information Systems, 22:443 - 458.

De Haes, S. & Van Grembergen, W. 2004. IT Governance and Its Mechanisms. Information Systems Audit and Control Association, 1.

Ferguson, C., Green, P., Vaswani, R. & Wu, G. 2013. Determinants of Effective Information Technology Governance. International Journal of Auditing, 17:75 - 99.

Gartner. 2006. Defining IT Governance: Roles and Relationships [Online]. Available: http://www.gartner.com [19 May 2013].

Gartner. 2009. IT Governance must be driven by Corporate Governance [Online]. Available: http://www.gartner.com [19 May 2013].

Gartner. 2010. Executive Summary: Practical Governance [Online]. Available: http://www.gartner.com [29 October 2012].

Gartner. 2011. Coherent Action is a competitive advantage: How can CIO's help [Online]. Available: http://www.gartner.com [10 June 2012].

Gartner. 2012a. Updates in COBIT 5 aim for greater relevance to wider business audience [Online]. Available: http://www.gartner.com [28 September 2013].

Gartner. 2012b. Define Governance from a Corporate objectives perspective [Online]. Available: http://www.gartner.com [29 October 2012].

Goosen, R. 2011. The development of an integrated framework in order to implement information technology governance principles at a strategic and operational level for medium- to large sized South African businesses. Unpublished master's dissertation. Stellenbosch: University of Stellenbosch.

Institute of Directors Southern Africa (IODSA). 2009a. King Report on Corporate Governance for South Africa (KINGIII). Pietermaritzburg: Interpak Books.

Institute of Directors Southern Africa (IODSA). 2009b. King Code of Corporate Governance for South Africa (KINGIII). Pietermaritzburg: Interpak Books.

ISACA. 2012. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT [Online]. Available: http://www.isaca.org [25 July 2012].

IT Governance Institute (ITGI). 2003. Board Briefing on IT Governance, 2nd edition [Online]. Available: http://www.itgi.org [26 September 2013].

JSE Limited. 2011. JSE Limited Listing Requirements: Service Issue 14. Johannesburg: LexisNexis.

Luftman, R., Rapp, R. & Brier, T. 1999. Enablers and inhibitors of Business-IT alignment. Communications of the Association for Information Systems, 1:1 - 33.

Weill, P. & Ross, J.W. 2004a. IT Governance on One Page [Online]. Available: http://www.web.mit.edu/cisr/www [21 September 2013].

Weill, P. & Ross, J.W. 2004b. IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. Boston: Harvard Business School Press.

Stellenbosch University http://scholar.sun.ac.za

Appendix A: De Haes and Van Grembergen (2008:449) validated list of IT governance practices mapped to the IT governance principles of KINGIII (IODSA, 2009a)

De Haes and Van Grembergen validated list of Information Technology Governance (ITG) practices (De Haes & Van Grembergen, 2008:449)			**KINGIII ITG PRINCIPLES (IODSA, 2009a)**							**Count of P**	**Count of S**	**Count of K3**
			Principle 1	**Principle 2**	**Principle 3**	**Principle 4**	**Principle 5**	**Principle 6**	**Principle 7**			
Structure (S), process (P) or relational mechanism (M)	**Description** of ITG structure, process or relational mechanism	**Definition** of ITG structure, process or relational mechanism	The board should be responsible for ITG	IT should be aligned with the performance and sustainability objectives of the company	The board should delegate to management the responsibility for the implementation of an ITG framework	The board should monitor and evaluate significant IT investments and expenditure	IT should form an integral part of the company's risk management	The board should ensure that information assets are managed effectively	A risk committee and audit committee should assist the board in carrying out its IT responsibilities			
S	**IT strategy committee at level of board of directors**	**Committee at level of board of directors to ensure IT is regular agenda item and reporting issue for the board of directors**	**P**	**P**	**P**	**P**		**P**		**5**	**0**	**0**

Stellenbosch University http://scholar.sun.ac.za

S	IT expertise at level of the board of directors	Members of the board of directors have expertise and experience regarding the value and risk of IT	P	P	P	P	P	P		6	0	0
S	(IT) audit committee at level of board of directors	Independent committee at level of board of directors overviewing (IT) assurance activities	P		S	S; K3 (d)	S	S	P; K3 (d)	2	4	2
S	**CIO on executive committee**	**CIO is full member of the executive committee**		**P**	**P; K3 (d)**	**S**	**S**	**P**		**3**	**2**	**1**
S	**CIO reporting to CEO and/or COO**	**CIO has direct reporting line to the CEO and/or COO**		**P**	**P; K3 (d)**	**S**	**S**	**P**		**3**	**2**	**1**
S	**IT steering committee (IT investment evaluation / prioritisation at execution / senior management level)**	**Steering committee at executive or senior management level responsible for determining business priorities in IT investments**		**P**	**P; K3 (d)**	**P**		**S**		**3**	**1**	**1**

Stellenbosch University http://scholar.sun.ac.za

S	ITG function / officer	Function in the organisation responsible for promoting, driving and managing IT governance processes		P	P	S	S	S		2	3	0
S	Security / compliance / risk officer	Function responsible for security, compliance and/or risk, which possibly impacts IT			S		P			1	1	0
S	**IT project steering committee**	**Steering committee composed of business and IT people focusing on prioritising and managing IT projects**			**S**	**P**		**S**	**S**	**1**	**3**	**0**
S	IT security steering committee	Steering committee composed of business and IT people focusing on IT related risks and security issues			S		P		P; K3 (d)	2	1	1

Stellenbosch University http://scholar.sun.ac.za

S	Architecture steering committee	Committee composed of business and IT people providing architecture guidelines and advise on their applications		S	S	P		S		1	3	0
S	Integration of governance / alignment tasks in roles & responsibilities	Documented roles & responsibilities include governance / alignment tasks for business and IT people		P	P	S	S	S		2	3	0
P	**Strategic information systems planning**	**Formal process to define and update the IT strategy**	**P**	**P; K3 (d)**	**S**	**P**	**S**	**S**		**3**	**3**	**1**
P	IT performance measurement (e.g. IT balanced scorecard)	IT performance measurement in domains of corporate contribution, user orientation, operational excellence and future orientation		S	S	P		P		2	2	0

Stellenbosch University http://scholar.sun.ac.za

P	**Portfolio management (incl. business cases, information economics, ROI, payback)**	**Prioritisation process for IT investments and projects in which business and IT is involved (incl. business cases)**		**S**	**S**	**P; K3 (i)**		**P**		**2**	**2**	**1**
P	Charge back arrangements – total cost of ownership (e.g. activity based costing)	Methodology to charge back IT costs to business units, to enable an understanding of the total cost of ownership				P		S		1	1	0
P	Service level agreements	Formal agreements between business and It about IT development projects or IT operations		S	S	S	S	P		1	4	0
P	IT governance framework COBIT	Process based IT governance and control framework	P; K3 (i)	S	P	P	P; K3 (i)	P; K3 (i)	S	5	2	3
P	IT governance assurance and self-assessment	Regular self-assessments or independent assurance activities on the governance and control over IT		S	S	P	S	S	P	2	4	0

Stellenbosch University http://scholar.sun.ac.za

P	**Project governance / management methodologies**	**Process and methodologies to govern and manage IT projects**	**P**		**S**	**P; K3 (d)**				**2**	**1**	**1**
P	**IT budget control and reporting**	**Process to control and report upon budgets of IT investments and projects**	**P**		**S**	**P**		**P**		**3**	**1**	**0**
P	Benefits management and reporting	Process to monitor the planned business benefits during and after implementation of the IT investments / projects				S		P		1	1	0
P	COSO / ERM	Framework for internal control			S		P	S	S	1	3	0
M	Job-rotation	IT staff working in business units and business people working in IT		S			S	P		1	2	0
M	Co-location	Physically locating business and IT people close to each other		S			S	P		1	2	0

Stellenbosch University http://scholar.sun.ac.za

M	Cross-training	Training business people about IT and / or training IT people about business		S			S	P		1	2	0
M	Knowledge management (on ITG)	Systems (intranet,…) to share and distribute knowledge about ITG framework, responsibilities, tasks, etc.		S			S	P		1	2	0
M	Business / IT account management	Bridging the gap between business and IT by means of account managers who act as in-between		S			S	P		1	2	0
M	Executive / senior management giving the good example	Senior business and IT management act as “partners”		P			S	P		2	1	0

Stellenbosch University http://scholar.sun.ac.za

M	Information meetings between business and IT executives / senior management	Information meetings, with no agenda, where business and IT senior management talk about general activities, directions, etc. (e.g. during informal lunches)		P			P	P		3	0	0
M	**IT leadership**	**Ability of CIO or similar role to articulate a vision for IT's role in the company and ensure that this vision is clearly understood by managers throughout the organisation**	**P**	**P**	**P; K3 (i)**	**S**		**P**		**4**	**1**	**1**
M	Corporate internal communication addressing IT on a regular basis	Internal corporate communication regularly addresses general IT issues		S	S		S	S		0	4	0

Stellenbosch University http://scholar.sun.ac.za

M	ITG awareness campaigns	Campaigns to explain to business and IT people the need for ITG	P	S	S		S	S		1	4	0

KEY	
K3 (i)	The structures, processes or relational mechanisms cross referenced to the principles of KINGIII with this key, are referred to in KINGIII in an **indirect** manner. I.e. the concept is discussed, but the specific structure, process or relational mechanism is not referred to directly.
K3 (d)	The structures, processes or relational mechanisms cross referenced to the principles of KINGIII with this key, are referred to in KINGIII in a **direct** manner.
P	The structures, processes and relational mechanisms cross referenced to the principles of KINGIII with this key, indicates that the specific structure, process or relational mechanism can be used to **directly** address the objectives of the related KINGIII principle.
S	The structures, processes and relational mechanisms cross referenced to the principles of KINGIII with this key, indicates that the specific structure, process or relational mechanism can be used to **indirectly** address the objectives of the related KINGIII principle.
	Lines highlighted in this colour represent the minimum baseline structures, processes and relational mechanisms identified by De Haes, S. and Van Grembergen, W. in the context of the attributes of perceived effectiveness and ease of implementation, together with professional experience and day-to-day practice, specifically for the Belgian financial services sector.

This table was compiled from information contained in the table of validated IT governance practices compiled by De Haes and Van Grembergen (2004:449), the King Report on Governance for South Africa 2009 (IODSA, 2009b) and the King Code of Governance for South Africa 2009 (IODSA, 2009a). The mapping of the IT governance practices to the IT governance principles was done by the researcher.

Appendix B: Cragg et al. (2011:357) framework of organizational IS competences in SME's mapped to the IT governance principles of KINGIII (IODSA, 2009a)

A framework of organizational IS competences in SME's developed by Cragg et al. (2011:357)			KINGIII ITG PRINCIPLES (IODSA, 2009)						
			Principle 1	**Principle 2**	**Principle 3**	**Principle 4**	**Principle 5**	**Principle 6**	**Principle 7**
Macro competence	**Competence**	**The ability to…**	The board should be responsible for ITG	IT should be aligned with the performance and sustainability objectives of the company	The board should delegate to management the responsibility for the implementation of an ITG framework	The board should monitor and evaluate significant IT investments and expenditure	IT should form an integral part of the company's risk management	The board should ensure that information assets are managed effectively	A risk committee and audit committee should assist the board in carrying out its IT responsibilities
Business and IS strategic thinking	IS innovation	recognise business opportunities from current and emerging hardware and software applications. Ideas can come from IS suppliers, employees, competitors, clients, consultants or other business.		x		x			
	Business case and investment criteria	define a business case and establish appropriate criteria for decision making on IS investments.				x			
	Including IS in business strategy	incorporate current and new IS into plans for the business, including an IS budget or a willingness to invest in IS.	x	x					
	Information governance	define information management policies and review the effectiveness of IS within the organization, including IS value, policies, roles and responsibilities of general management and any IS staff.	x		x	x		x	x

Stellenbosch University http://scholar.sun.ac.za

Define IS contribution	IS alignment	change (or stabilize) the IS programme according to business priorities to ensure IS plans are integrated with organizational needs or business strategy.	x	x					
	Business Process Management	design and improve business processes of the organization.		x	x		x	x	
	Define information system requirements	define appropriate business requirements for software applications.			x	x			
	Accessing IS knowledge	identify appropriate people (within or outside the firm), organizations and secondary information sources (e.g. internet, books, conferences, etc.) to seek guidance on IS issues.			x				
Define the IS strategy	Software sourcing strategies	define appropriate software sourcing strategies, for example: package acquisition, in-house development, contract-out, outsource.		x	x	x			
	IS acquisition processes	establish criteria and processes to evaluate supply chain options and contracts with IT suppliers.			x	x			
	Technology infrastructure requirements	identify and develop appropriate hardware infrastructure requirements.		x					
Exploitation	Benefits management	explicitly identify, plan and evaluate the benefits derived from IS investments and use.				x			
	Managing change	make the business and organizational changes required to maximise the benefits of IS adoption. It requires top management commitment and often top management involvement, to involve others.			x				
	Project management	manage project scope, resources and time, through planning, organizing and controlling, usually involving multidisciplinary teams.			x	x			

Stellenbosch University http://scholar.sun.ac.za

	Inter-organizational collaboration	develop collaborative alliances and work with business partners (e.g. customers and suppliers) to enable external IS integration.		x	x				
Deliver solutions	Applications development	develop or customise in-house software applications that satisfy business needs.		x	x				
	Implementation and integration	implement and integrate IS that satisfies business needs.		x	x				
	Apply and use technology	use computers and develop IS skills by managers and other users in the organization.			x				
	Business continuity and security	provide effective recovery, contingency and security processes to prevent risk of business failure.			x		x		x
Supply	Manage IS supplier relationships	develop value added relationships between the business and IS suppliers (external and internal), including service level agreements and contract management (performance monitoring, problem resolution and negotiating amendments).			x	x			
	Information asset management maintenance	ensure technology, data and application assets are effective. This requires that they are viewed and maintained. It includes, for example, controls and procedures for the use of IS, costs, operational policies for network management and data quality.		x		x			
	Staff development	recruit, train and deploy appropriate staff and ensure technical, business and personal skills meet the IS needs of the organization.		x	x	x	x	x	

Stellenbosch University http://scholar.sun.ac.za

KEY	
x	The competence described by Cragg et al. (2011:357) can be utilised to address the IT governance principles set out in KINGIII (IODSA, 2009a).

This table was compiled from information contained in framework of organizational IS competences in SME's compiled by Cragg et al. (2011:357), the King Report on Governance for South Africa 2009 (IODSA, 2009b) and the King Code of Governance for South Africa 2009 (IODSA, 2009a). The mapping of the IS competences to the IT governance principles was done by the researcher.

Appendix C: Cragg et al. (2011:357) framework of organizational IS competences in SME's mapped to the Five Key IT Decisions of Weill and Ross (2004b:25 – 49)

A framework of organizational IS competences in SME's developed by Cragg et al. (2011:357)			Five Key IT Decisions: making IT a strategic asset (Weill & Ross, 2004b:25 - 49)				
			Decision 1	**Decision 2**	**Decision 3**	**Decision 4**	**Decision 5**
Macro competence	**Competence**	**The ability to…**	IT Principles	IT Architecture	IT Infrastructure	Business application needs	IT investment and prioritization
Business and IS strategic thinking	IS innovation	recognise business opportunities from current and emerging hardware and software applications. Ideas can come from IS suppliers, employees, competitors, clients, consultants or other business.			x	x	
	Business case and investment criteria	define a business case and establish appropriate criteria for decision making on IS investments.	x	x	x		x
	Including IS in business strategy	incorporate current and new IS into plans for the business, including an IS budget or a willingness to invest in IS.	x				x
	Information governance	define information management policies and review the effectiveness of IS within the organization, including IS value, policies, roles and responsibilities of general management and any IS staff.		x	x		
Define IS contribution	IS alignment	change (or stabilize) the IS programme according to business priorities to ensure IS plans are integrated with organizational needs or business strategy.	x				x
	Business Process Management	design and improve business processes of the organization.		x	x	x	

Stellenbosch University http://scholar.sun.ac.za

	Define information system requirements	define appropriate business requirements for software applications.				x	
	Accessing IS knowledge	identify appropriate people (within or outside the firm), organizations and secondary information sources (e.g. internet, books, conferences, etc.) to seek guidance on IS issues.			x		
Define the IS strategy	Software sourcing strategies	define appropriate software sourcing strategies, for example: package acquisition, in-house development, contract-out, outsource.	x	x	x	x	
	IS acquisition processes	establish criteria and processes to evaluate supply chain options and contracts with IT suppliers.			x		x
	Technology infrastructure requirements	identify and develop appropriate hardware infrastructure requirements.		x	x		
Exploitation	Benefits management	explicitly identify, plan and evaluate the benefits derived from IS investments and use.			x		
	Managing change	make the business and organizational changes required to maximise the benefits of IS adoption. It requires top management commitment and often top management involvement, to involve others.			x		
	Project management	manage project scope, resources and time, through planning, organizing and controlling, usually involving multidisciplinary teams.			x		
	Inter-organizational collaboration	develop collaborative alliances and work with business partners (e.g. customers and suppliers) to enable external IS integration.			x		
Deliver solutions	Applications development	develop or customise in-house software applications that satisfy business needs.	x		x	x	
	Implementation and integration	implement and integrate IS that satisfies business needs.	x	x	x		
	Apply and use technology	use computers and develop IS skills by managers and other users in the organization.			x	x	

Stellenbosch University http://scholar.sun.ac.za

	Business continuity and security	provide effective recovery, contingency and security processes to prevent risk of business failure.			**x**		
Supply	Manage IS supplier relationships	develop value added relationships between the business and IS suppliers (external and internal), including service level agreements and contract management (performance monitoring, problem resolution and negotiating amendments).			**x**		
	Information asset management maintenance	ensure technology, data and application assets are effective. This requires that they are viewed and maintained. It includes, for example, controls and procedures for the use of IS, costs, operational policies for network management and data quality.			**x**		
	Staff development	recruit, train and deploy appropriate staff and ensure technical, business and personal skills meet the IS needs of the organization.			**x**		

KEY	
x	The competence described by Cragg et al. (2011:357) can be utilised to address the key IT decision described by Weill and Ross (2004b:27 - 49).

This table was compiled from information contained in framework of organizational IS competences in SME's compiled by Cragg et al. (2011:357) and the Five Key IT Decisions introduced by Weill and Ross (2004b:25 – 49). The mapping of the IS competences to the IT governance principles was done by the researcher.