Beyond King III: Assigning accountability for IT governance in South African enterprises

R. Butler*
Department of Accounting, University of Stellenbosch,
Stellenbosch 7600, Republic of South Africa
rbutler@sun.ac.za

M.J. Butler
University of Stellenbosch Business School, PO Box 610,
Bellville 7535, Republic of South Africa
martin.butler@usb.ac.za

Received February 2010

With the increasing dependence on IT in modern enterprises and the significant risks associated with omnipresent IT systems in business, IT governance is becoming imperative to all organisations. King III is based on the "apply or explain" approach, that forces South African entities for the first time to apply the IT governance principles as contained in the report, or explain the reasons for not applying these principles. This paper provides a macrolevel view of IT governance, derived from King III, and determined that it correlates strongly with the growing body of knowledge on IT governance. The paper investigates the responsibilities for IT governance within organisations and provides clear guidelines on the responsibilities of management roles, from the board to the operational level, involved in IT governance to ensure accountability.

*To whom all correspondence should be addressed.

Introduction

The role of information technology (IT) in business has changed from an enabler of business to sufficiently pervasive to be "at the core of most organizations' ability to execute strategy" (Symons, 2005). IT has become an integral part of business and fundamental to support, sustain and grow an entity. The increasing importance and prominence of IT in business and entities' increasing dependency on IT made it necessary to pay special attention to IT (Damianides, 2005; De Haes & Van Grembergen, 2008). One attempt at managing this increasingly important relationship is the emergence of Information Technology Governance (ITG).

A global survey indicated a correlation between the state of advancement of ITG practices and the outcomes of IT, in particular the extent to which IT investments create value in the entity and the degree to which IT performs against expectations (ITGI, 2009a; ITGI, 2009b). Entities are driven towards ITG as a result of (Tarantino, 2008; Pultorak & Kerrigan, 2005; Damianides, 2005; Raghupathi, 2007):

- The search for competitive advantage through the way in which IT is used, thereby creating sustainable customer value and increasing company profits;
- The need to comply with evolving governance requirements, like those imposed by King III, as well as any regulatory and legal requirements such as increasing information and privacy related legislation;
- The increasing rise of threats to intellectual assets, information and IT in respect of availability, confidentiality and integrity of information assets and the need to address these risks;
- The need to align technological projects with strategic organizational goals to ensure that the expected value is delivered.

These developments ultimately resulted in the introduction of directives on "the governance of IT as a corporate imperative" for South African entities (IODSA, 2009).

The governance of IT was introduced in the Third King Report on Governance for South Africa (King III), issued by the Institute of Directors in Southern Africa (IODSA) on 1 September 2009 (King, 2009). King III came into effect for South African entities from 1 March 2010. As opposed to King I (issued 1994) and King II (issued 2002), King III is applicable to *all entities*, irrespective of their size and whether or not they are listed. The "apply or explain" basis of the King III report requires every entity to apply the King III principles as they best meet the objectives of the entity

concerned. The report supports the implementation of corporate governance principles regarding IT that are appropriate and applicable to an entity, taking into account aspects such as the entity's size, IT's role within the entity and any legal obligations (IODSA, 2009; Liell-Cock, Graham & Hill, 2009).

King III emphasises that "directors should ensure that prudent and reasonable steps have been taken in regard to IT Governance" (IODSA , 2009). Research indicated that one of the key factors distinguishing top-performing from standard-performing entities was the leadership and the level of involvement of management in making key IT decisions and the way in which IT supported the business (Kordel, 2004). Nonetheless, boards tend to pay insufficient attention to IT (Damianides, 2005) as they traditionally focus on aspects such as the business strategy, risks, return on investment (ROI) and financial and accounting issues. IT is often regarded as an entity "separate and distinct from the business" and not integrated into and managed with the rest of the business (Kordel, 2004). In addition, a lack of the necessary technology expertise is often evident (Damianides, 2005). Boards have "little interest" for technology issues and "even less expertise" regarding IT and tend to delegate IT-related aspects such as its governance to lower levels of management (Raghupathi, 2007). This is supported by the IT Governance Global Status Report (ITGI, 2008) where 58% of the respondents noted an insufficient number of staff, while 38% reported staff with inadequate skills to support the business effectively.

Many, if not most, directors "do not have a strong understanding of the controls issues raised by IT and do not even know what questions they should ask to place themselves in a position to address their responsibilities" (Trites, 2004). In addition, board members often find it difficult "to keep up with the rapid changes taking place in IT and, therefore, to know what questions to ask to ensure that IT issues are being properly addressed" (CICA, 2004). These facts and recent developments have made is critical for directors and managers of South African entities to familiarize themselves with their new roles and responsibilities in respect of ITG.

Study purpose, method and limitations

The primary objective of this study is to provide guidance on ITG accountability to individual management layers, a level of detail not addressed in King III, and neither adequately addressed within existing literature.

This study provides guidance to the management of South African entities that are required to apply King III's regulations regarding ITG, but wish to fully comprehend what ITG entails to ensure that they understand the control issues and also know the right questions to ask. It also provides clarity on the extent to which King III compliance will ensure proper utilisation of existing ITG best practices to ensure that the entity reaps maximum value from ITG, whilst adhering to the King III principles. An important concept, neither raised nor answered by King III, is who to ask these questions to.

The primary research question addressed by this paper is: *What are the appropriate organisational roles, and the corresponding ITG responsibilities, to ensure accountability for ITG within an organisation?* The secondary question, answered en route to this outcome, is: *To what extent does compliance to King III's ITG principles correlate with a comprehensive macrolevel view of ITG?* The answer to the primary research question provides guidance on ITG accountability and the secondary question, on the extent to which King III addresses the ITG domain.

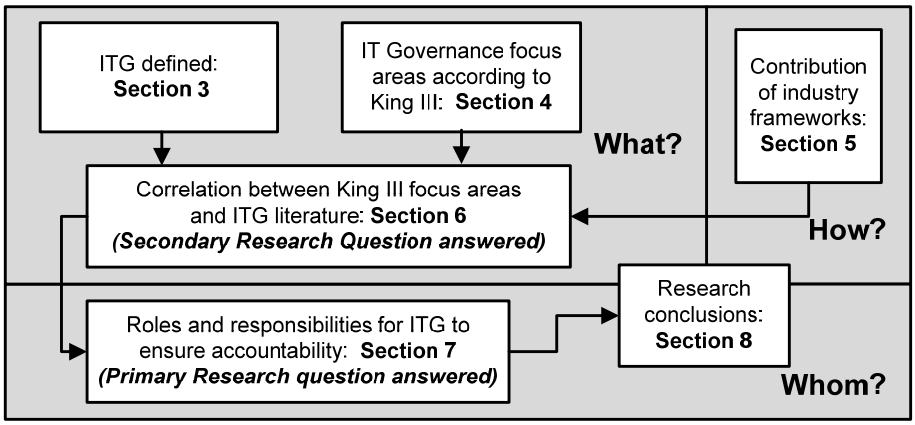

Figure 1: Research process

A literature review was used to clearly define Information Technology Governance (ITG) (Section 3). The King III principles on ITG as set out in Chapter 5 of the King Report were then analysed to compile ITG focus areas that provide a macrolevel description of ITG according to King III (Section 4). The role and limitations of industry frameworks were determined (Section 5), and the correlation of the King III focus areas with ITG literature was determined (Section 6) to answer the secondary research question.

In order to ensure accountability for ITG within organisations the typical organisation and IT management roles and responsibilities are presented and the ITG focus areas are mapped to the appropriate roles and

responsibilities for ITG (Section 7) to answer the primary research question, followed by the research conclusions (Section 8).

Various methods, methodologies, techniques, tools and frameworks exist within the field of ITG. The purpose of this research is not to discuss any one of these in detail, or to recommend the application of the one or the other. The objective is rather to explain where these frameworks fit into the process of ITG and to ensure clear accountability. In addition, the ITG focus areas derived within this article (Figure 2) is not presented as an optimum high-level view of ITG, but as an appropriate categorisation of ITG responsibilities that is suitable for the purpose used within this paper.

IT Governance defined

The IT Governance Institute (ITGI) defines Information Technology Governance (ITG) as "an integral part of enterprise governance" that consists of "the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives" (ITGI, 2003). An often cited definition of ITG is to understand the issues and the strategic importance of IT, so that the company can maintain its operations and implement strategies to enable it to better compete now and in the future (Chun, 2005). According to Chun (2005), ITG consists of the decision rights and accountability framework to encourage desirable behaviour in the use of IT. Another perspective is that ITG is in essence the process by which decisions regarding IT investments are made (Symons, 2005).

For the purpose of this study the following definition of Weill (2004), as cited by Brown and Grant (2005: 697) will be used: *"IT governance represents the framework for decision rights and accountability to encourage desirable behaviour in the use of IT"*.

According to De Haes and Van Grembergen (2008), ITG can be achieved by "using a mixture of processes, structures and relational mechanisms". When constructing a framework for ITG the following three elements should be considered (Symons, 2005; De Haes & Van Grembergen, 2008; Larsen, Pederson & Anderson, 2006):

a) Governance structures (*who makes the decisions and who is held accountable?)*: This is the organizational structure, roles, positions and responsibilities created within the entity in respect of the IT investment process. It includes reporting relationships and governance-specific positions created, such as committees with governance responsibilities.

b) Governance processes *(how decisions are made?)*: These include all the processes regarding governance that the above governance structures will be tasked to enforce based on the IT governance framework adopted by the entity.

c) Governance communication or relational mechanisms (*how the results of governance and IT decisions are monitored, measured and communicated?):* IT governance will only be effective if the related information is measured and communicated throughout the entity.

Although the industry standards and frameworks provide guidance on detail processes (b) and communications (c), a clear assignment of responsibilities (a) is not always covered adequately.

IT Governance according to King III

King III ITG principles and focus areas

According to King III, ITG should form "an integral part of the overall corporate governance" of an entity. It provides a framework (including the relevant structures, processes and mechanisms) that is the responsibility of the board. ITG should ensure that IT is integrated into the strategy of the entity in such a way that it adds value to the business and mitigates IT risks. IT should enable the improvement of the entity's performance and sustainability and support the effective and efficient management of IT resources to facilitate the achievement of a company's strategic objectives (IODSA, 2009).

Chapter 5 of King III (IODSA, 2009) contains seven principles for ITG, with accompanying recommendations for South African entities to apply, as indicated in Table 1.

Table 1: Seven IT Governance principles of King III

Principle	Description
Principle 5.1	The board should be responsible for information technology governance
Principle 5.2	IT should be aligned with the performance and sustainability objectives of the entity
Principle 5.3	The board should delegate the responsibility for the implementation of an IT Governance framework to management
Principle 5.4	The board should monitor and evaluate significant IT investments and expenditure
Principle 5.5	IT should form an integral part of the entity's risk management process
Principle 5.6	The board should ensure that information assets are managed effectively
Principle 5.7	A risk committee and audit committee should assist the board in carrying out its IT responsibilities

From the above the following important deductions can be made regarding ITG, as seen by King III:

- Where does the responsibility for ITG lie? (*Whom?*): ITG is the responsibility of the board (principle 5.1), who should delegate relevant responsibilities to management and appropriate subcommittees of the board (principles 5.3 and 5.7).

- How is ITG achieved? (*How?*): ITG consists of a framework with relevant structures, processes and

mechanisms that should be integrated into the corporate strategy (principle 5.3).

- What are the objectives of ITG? (*What?*): The objectives of ITG can be stated as:
    - Managing IT resources effectively and efficiently to ensure the achievement of strategic objectives (principle 5.6) – **Resource management and Strategic alignment**;
    - Ensuring that IT-related risks are appropriately mitigated (principle 5.5) – **Risk management**;
    - Enabling the improvement of the organisation's performance and sustainability (principle 5.2) – **Performance management**;
    - Monitoring and evaluating the investment in IT to ensure it delivers value (principle 5.4) – **Value delivery**.

From the King III principles for ITG the authors derived the key focus areas for ITG that provide a macrolevel overview of the concept (Figure 2).

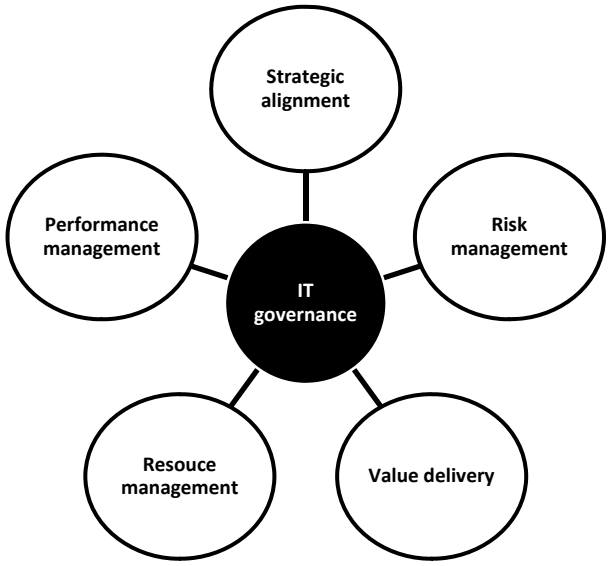

Figure 2: IT Governance focus areas according to King III

Based on the literature review (ITGI, 2003; Hardy, 2003; Kordel, 2004; Chun, 2005; Symons, 2005; Brisebois, Boyd & Shadid, 2010), the five focus areas of ITG indicated can be described as follows:

- **Strategic alignment** follows from a shared understanding of strategic imperatives between the organisation's management and the IT department. It also enables management (and the board) to understand strategic IT issues. The IT investments are aligned with the overall strategies of the organisation.

- **Resource management** ensures that IT has sufficient, competent and efficient resources, human and equipment, to meet the organisation's demands.

- **Risk management** ensures that the organisation and IT regularly assess and report IT-related risks and its organisational impact within the risk management strategy of the organisation. IT risks are categorised according to business impact and not the impact to IT operations.

- **Value delivery** requires a valid business case for each IT investment and the measurement of benefits realised postimplementation to ensure that the investment delivers value to the organisation.

- **Performance management** encapsulates the concept of efficiency (mostly IT operations) and effectiveness (mostly IT projects) to ensure accurate, timely and relevant performance information to senior management. Once reported on, and compared with either a baseline or an established norm, performance management includes appropriate actions according to the measured variations.

This article does not proclaim to define these areas for the first time, quite the contrary. Table 3 indicates that the focus areas derived from King III and presented in Figure 2 is strongly evident in the published ITG theory and referred to by many other authors.

Application of King III focus areas within business

In order to determine the management responsibilities for each of the focus areas of ITG, it is necessary to understand the relationship between the IT infrastructure of an organisation, the core business processes that represent the value added by the business, and its strategy and resources. Since the objective of any business entity is achieving its objectives with the effective and efficient use of resources, including the IT infrastructure, the five focus areas for ITG should ideally ensure that this is indeed the case.

Efficiency and effectiveness are central terms used in assessing and measuring the performance of organisations. It is important to distinguish between the strategic responsibility, which would in most instances relate to the effectiveness, ensuring the correct application of IT resources, and the operational responsibility that needs to ensure an efficient use of IT resources.

In the management literature, efficiency is often associated with performing activities correctly, or "doing things right", whereas effectiveness is often equated with the proper selection of the activities or "doing the right things" (Drucker, 1977; Griffin, 1987). Based on the research by Mouzas (2006), Drucker (1977) and Kao, Chen, Wang, Kuo and Horng (1995), the two concepts can be defined as follows:

- Effectiveness relates to achieving the stated objectives; it thus pertains to a strategic intent and the alignment of the IT resources with this strategic intent.

- Efficiency relates to ensuring that the correct resources are available to deliver a service, including the extent

to which the IT resources are consumed to deliver the service.

The accountability for this rather complex concept of efficient and effective management of IT resources thus requires the attention of different levels of management within an organisation. At the strategic level (effectiveness) IT should be aligned to the strategic objectives of the entity, while at the operational level (efficiency) IT should support and add value to the entity and improve the entity's performance while consuming the minimum amount of resources.

Figure 3 shows the relationship between the organisation's strategy and objectives, the core business operations (producing goods and services and delivering these to clients), IT infrastructure and the organisational resources consumed by business operations.

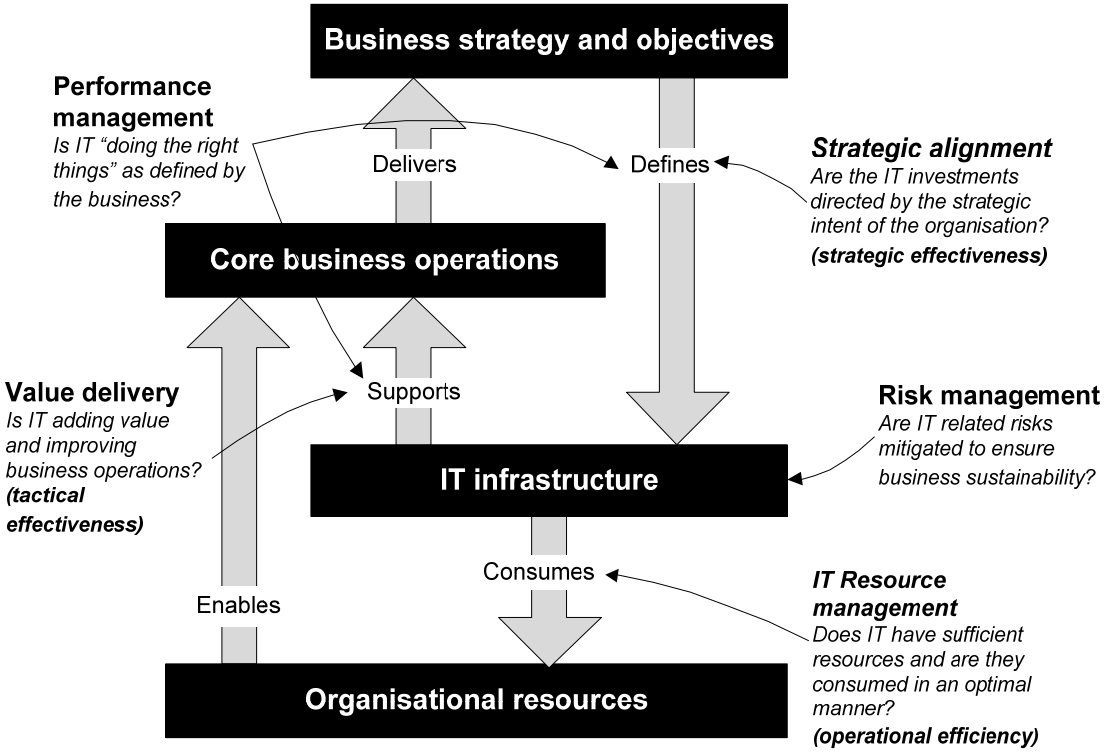

Figure 3: ITG focus areas and business architecture

By mapping the ITG focus areas to the key business areas (Figure 3) it becomes evident that different management levels and roles are involved in ensuring enterprise-wide ITG. For any organisation venturing into ITG the focus areas identified in this document represent a comprehensive starting point. Although various frameworks all contribute at microlevel, it is the understanding of these concepts at the macrolevel that ensures a comprehensive ITG strategy, supported by an appropriate framework.

IT Governance frameworks

King III refers to frameworks that may be used to assist in an entity's IT governance efforts (principle 5.3). There is a fair number of supporting references (or frameworks) available to guide the implementation of ITG (Brown & Grant, 2005). Despite the existence of multiple frameworks a global study, that included South Africa, indicated that 57% of the respondents were not familiar with any kind of standard or framework to provide guidance in governing IT (ITGI, 2008). In addition, 55% of the respondent entities used external advisors as their leading source of ITG due to their own lack of knowledge (ITGI, 2009a). A literature review revealed that the following IT-focused frameworks and standards are the most widely recognized (Table 2).

The Information System Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) rated the highest amongst the ITG solution providers in the IT Governance Global Status Report for 2008. The report also indicated that CobiT, ITIL and ISO are the most popular formal IT governance frameworks applied by entities (ITGI, 2008).

Nonetheless, King emphasises, and is strongly supported by Tarantino (2008) and Symonds (2005), that a "one size fits all" approach is not possible (IODSA, 2009). There is "no silver bullet" for the implementation of ITG that will be suited to every entity (Tarantino, 2008). Factors such as the industry's ethics, the entity's structure, culture, mission, vision and strategy are all factors that influence the ITG environment, and which should be considered when designing an appropriate framework for IT governance (Symons, 2005; Kordel, 2004).

Table 2: Most popular IT governance frameworks

Framework	Description	Main focus
CobiT	The Control Objectives for Information and Related Technology was first published in 1996 and is now in its fourth version. It was originally created by the Information Systems Audit and Control Association (ISACA) and is now the responsibility of the IT Governance Institute (ITGI).	This framework provides control over information, IT and related risks and is primarily a risk management and compliance framework. It contains 34 high-level objectives, covering 215 control objectives, grouped into four domains. With these objectives entities can assess and measure the performance of IT within their entities. It is generic, process-based and has a strong bias towards auditability (Damianides, 2005; Symons, 2005; Pultorak & Kerrigan, 2005).
IS0 27002:2005 (previously ISO 17799)	The Code of Practices for Information Security Management was published by the International Organization for Standardization (ISO) and the International Engineering Consortium (IEC). ISO 17799 was first published in 2005.	IS0 27002:2005 is an information security standard that provides best practice recommendations for 12 key information security areas (Symons, 2005; Calder, 2008).
ISO 27001: 2005		ISO 27001 provides a system against which information security management systems can be certified (Calder, 2008).
ITIL	The IT Infrastructure Library was published by the Central Computer and Telecommunications Agency (CCTA), now the British Office of Government Commerce (OGC).	An IT management framework in a series of eight books that provides best practice recommendations for managing IT service levels and delivery in line with the business' requirements. It is particularly process-oriented (Symons, 2005; Pultorak & Kerrigan, 2005; Calder, 2008).
ISO 20000: 2006	The international standard for IT service management as a standard for the provision of IT services.	A framework heavily based on ITIL and the world's first standard for IT service management (Disterer, 2009; Calder, 2008).
ISO 38500:2008	A new international standard for the corporate governance of information and communications technology issued by the International Organization for Standardization (ISO).	A standard that provides guidance to boards and explains how they should address the responsibility in this regard (Calder, 2008).
Val IT	Developed by the Information Systems Audit and Control Association (ISACA).	A framework for the governance of IT investments (Calder, 2008).

Although no comprehensive ITG framework that fully meets all the requirements of IT governance exists, various ITG frameworks that provide a model for governing IT and comprising various definitions and principles are available. These frameworks can be applied by an entity as a starting point for developing and adopting an ITG framework suitable for that particular entity. Each of the frameworks has different strengths and weaknesses as well as overlaps.

Organisations are advised to review the frameworks that are available and may choose to either adopt an existing framework, to develop a framework of their own or use a combination of the two (Larsen, *et al.*, 2006). It may even be useful for entities to deploy different components of various frameworks as part of an entity's integrated and comprehensive framework, but within an appropriate macrolevel view. According to Spafford (as cited by Larsen, *et al.*, 2006), adopting an existing standard ITG framework will deliver benefits such as that the framework provides a structure that the entity can follow, based on best practices that have been developed over time and were assessed by numerous entities worldwide. The benefits of framework integration include a reduction in internal costs, improved compliance and better alignment (Calder, 2008).

Correlation between King III and ITG literature

Brown and Grant (2005) reviewed a significant number of ITG articles to create what they refer to as a "Conceptual Framework for IT governance research". The proposed framework contains two broad streams:

- IT Governance forms that deal with "decision-making structures adopted by IT organisations";
- IT Governance contingency analysis that contains "research focussing on the why and how of IT Governance fit".

The work of Brown and Grant (2005), although commendable and one of the most representative studies of ITG to date, offers little value to the practitioner. It serves as a broad structure of ITG research for future academic work. Similarly, Larsen, *et al*. (2006) who reviewed 17 ITG frameworks and created a grid (using process types and organisational entities) to categorize current ITG knowledge sets, offer little in terms of high-level focus areas, or applicable knowledge for the practitioner. In fact, it is stated by Jordan and Musson (2004) that "a gap exists between theoretical frameworks and contemporary practice" in ITG.

A number of authors do, however, define macrolevel principles or objectives for ITG that can be used to make a correlation between the focus areas derived from King III in Section 4 and the existing ITG body of knowledge. Table 3 contains the derived King III focus areas, together with the authors referring to these focus areas.

Table 3: IT Governance focus areas and key concepts emphasized by authors

Focus area	ITGI (2003)	Hardy (2003)	Kordel (2004)	Chun (2005)	Symons (2005)	Brisebois, Boyd & Shadid (2010)
Strategic alignment	*"IT strategic alignment"*	*"Strategic alignment"*	*"IT strategic alignment"*	*"… guide IT initiatives …"*	*"… alignment between the business units and IT …"*	*"Strategic alignment"*
Risk management	*"Risk management"*	*"Risk management"*	*"Risk management"*	*"...identification and management of IT-related risks …"*	*"Risk management"*	*"Risk management"*
Performance management	*"Performance measurement"*	*"Performance management*	*"Performance measurement"*	*"… ensure that performance meet corporate objectives …"*	*"Performance measurement"*	*"Performance management"*
Resource management	-	*"IT Resource management"*	*"IT Resource management"*	*"… responsible use of IT resources …"*	–	*"Resource management"*
Value delivery	*"IT value delivery"*	*"Value delivery"*	*"IT value delivery"*	–	*"Delivering value to the business …"*	*"Value delivery"*

The mapping of the key concepts of ITG with the focus areas derived from King III (Table 3) indicates (i) a direct correlation between the focus areas defined; and (ii) confirmation that the key concepts promulgated by King III indeed addresses all the focus areas of ITG identified in the literature.

The secondary research question of this study, namely to determine whether King III provides full coverage of the key concepts of ITG, can thus be answered in the affirmative. The focus areas derived from King III in Section 4 will thus be used as a theoretical base moving forward in determining where the accountability for ITG within the organisation resides.

Organisational roles and core responsibilities for ITG within organisations

Accountability for ITG

According to Luo (2005), "Accountability is both a key element of as well as a requirement for corporate governance". Accountability, as opposed to responsibility, which is the moral sense of duty, assumes "institutional authority to call an individual or group to account for their actions" (Leong, 1991). Although the management of IT must be linked directly "to the highest executive levels" of management within an entity (CICA, 2004), ITG activities "usually transcend management layers" (Damianides, 2005). It is thus essential to know which levels of management are accountable for ITG.

The King III principles states that the overall responsibility for ITG resides with the board (principle 5.1), who in turn should delegate relevant responsibilities to management roles (principles 5.3) and appropriate committees (principle 5.7). This is supported by the deductions made by Weill and Ross (2004) when they presented their *Ten Principles of IT Governance*. In their list Weill and Ross devotes two principles to the concept of accountability:

- Assigning or delegating ownership and accountability for ITG;
- IT Governance should be situated at various organizational levels within an entity.

The first principle emphasizes the fact that ownership needs to be clearly assigned to achieve accountability, rather like financial asset governance is assigned to the Chief Financial Officer (CFO). According to Weill and Ross (2004), three important issues should be considered when assigning ownership for ITG:

- ITG cannot be assigned in isolation from other organizational aspects, since those assigned "must have an enterprise-wide view that goes beyond IT", as well as a level of credibility with management;
- Those assigned cannot implement ITG alone; the "board or CEO must make it clear that all managers are expected to contribute to IT governance";
- Since IT assets are very important, the "person or group owning IT governance must understand what the technology is and is not capable of."

The second principle states that it is necessary to consider IT governance at several levels, especially in larger organizations. Although the starting point is enterprise-wide ITG driven by a number of enterprise-wide strategies and goals, the demand for synergy decreases at the lower levels within the organisation that might deploy and use IT differently (Weill & Ross, 2004).

This allows for different ITG approaches at lower levels within the same organisation. It is thus conceivable that different business functions, or even geographical deployments of the same business with varying degrees of IT exposure, could apply the principles of ITG differently. The outcome, however, should be the same for the

organisation as a whole; hence the importance of accountability.

With different levels of management involved in ITG, clearly assigned roles and responsibilities for these managers linked to each of the ITG focus areas is required to ensure accountability for the governance of IT.

Various levels of management involved in ITG

With the increased focus on ITG "top management issues for the oversight of IT have moved from technology to management-related areas" (Pultorak & Kerrigan, 2005). King III does not assign responsibility to individual management layers, but specifically mentions the following managerial parties as having a role to play regarding ITG: executive and IT management, the Chief Executive Officer (CEO), Chief Information Officer (CIO), the IT steering committee, the risk committee and the audit committee.

According to Weill and Ross (2004), the CIO owns ITG in most entities, while other organizations make the Chief Operating Officer (COO), the CEO, or a committee responsible for IT governance (CICA, 2004). An important finding from the research by Weill and Ross is that no single approach delivers the best results in all circumstances.

There is agreement, and it is also evident from the arguments presented, that ITG should be situated at multiple layers within an entity, and these levels, all with different responsibilities towards ITG, are defined as follows (De Haes & Van Grembergen, 2008):

- Strategic level (the involvement of the board of directors);
- Tactical management level within the C-suite layers (CEO, COO, CFO, CIO ...);
- Operational level (IT and business management).

Since ITG requires co-operation between strategic, tactical and operational management levels, it is important to determine exactly what these parties are accountable and responsible for with regard to ITG.

Strategic management

It is essential that the board and executive management "extend their governance responsibilities to IT" (Kordel, 2004). Boards should assume their responsibility for ITG (IODSA, 2009; ITGI, 2003) and need to understand the strategic importance of IT and put ITG firmly on their agenda (Kordel, 2004). Besides determining the decision rights and accountability framework of the entity (Liell-Cock, *et al.*, 2009), the board is responsible for clarifying the strategies and objectives of the business and clearly defining the role of IT in achieving them.

To achieve the practices recommended in King III the board should provide the required leadership and direction to ensure proper ITG and cultivate and promote ethical IT governance and management culture, awareness and a common IT language (IODSA, 2009). In addition, the board should ensure that an IT governance charter and policies and an appropriate IT internal control framework is adopted and implemented and that independent assurance on the effectiveness thereof is received (IODSA, 2009; Liell-Cock, *et al.*, 2009).

The most comprehensive work to date that covers the role of boards specifically, with respect to ITG, is the work of Buckby, Best and Stewart (2005). In taking ownership for ITG and providing leadership and direction the board should perform an effective oversight function with regard to management (Trites, 2004) and thus address all the focus areas identified earlier when the board:

- Provide the necessary guidance to management and ensure that an effective strategic planning process is in place to ensure that IT initiatives are aligned with real business needs and that the IT organisational structure complements the business model and direction **(Strategic alignment)**;
- Ensure that management has put adequate processes and practices in place to enable IT to deliver value to the business **(Value delivery)**;
- Monitor the way in which management determines the resources required to support operations and thus ultimately achieves the strategic goals, whilst also ensuring that IT investments are adequate to sustain and grow the entity **(IT Resource management)**;
- Challenge management's activities regarding IT to ensure that IT risk exposures are identified and addressed and that IT initiatives represent a balance between risk and reward **(Risk management)**;
- Assess IT management's performance measurement procedures and report thereon and work with the executives to define and monitor high-level IT performance **(Performance management)**.

The board should ensure that IT is placed on its agenda and ensure that the necessary resources are available to ensure that comprehensive IT reporting takes place, both to the board by management and by the board in the integrated report to all stakeholders. It is important that management report on the IT function at every board meeting (IODSA, 2009).

Trites (2004) questions whether the board has the necessary expertise to evaluate whether appropriate and effective procedures regarding ITG are in place. However, just as a board member is required to be literate about basic marketing, financial, operational and strategic terminology to partake in strategic debates and direction-setting and thus fulfil their duties, board members must have a basic comprehension of the key IT (and governance) concepts and terminology. In fact, board members without a basic comprehension of the role of the IT function, or governance for that matter, should be exposed to the key concepts that they are responsible for as part of a comprehensive ITG process.

Tactical management

The CEO should appoint a suitably qualified person as CIO for the management of IT (IODSA, 2009). The CIO has an extensive list of responsibilities and should act as a conduit between IT and the business. Mullins and Klinowski (2003), in defining the difference between the CIO and the Chief Technology Officer (CFO), states that the "CIO is responsible for ensuring that the company's information technology investments are aligned with its strategic business objectives. To this end, the CIO has emerged as the key executive for information assets, operations, and policy".

King III recommends that the CIO should have access to the board and regularly meet with the board (or appropriate board committee and executive management) on strategic IT matters (IODSA, 2009). This view is supported by the ITGI (2009a) that recommends that the CIO reporting line to top executive management should be "as direct as possible".

The CIO should be responsible for the implementation and execution of ITG within most entities. The CIO will be expected to implement the necessary structures, processes and governance mechanisms for the effective and efficient management of information resources to facilitate the achievement of corporate objectives. These responsibilities include understanding the accountability and responsibility for IT, as well as the following duties that relate to **strategic alignment**: to understand the business requirements and strategy and have the ability to translate the strategy and objectives into efficient and effective IT solutions, as well as to facilitate the integration of IT into the business strategy.

The tactical management layer does, however, extend far beyond the CIO into every business function of the enterprise where it is involved in **performance management**. It is impossible for the CIO to provide guidance on the 'correct activities' to ensure effectiveness in isolation. Although the CIO is the business executive charged with mapping IT initiatives to the goals of the organisation, it is important that all other functional departments (Operations, Marketing, Human Resources) are tied into the ITG process to ensure that the 'correct' business requirements for the Information Systems are defined and aligned to.

Whereas the strategic level management defines the high-level objectives, the tactical level defines the details of how the business will execute its processes to achieve these objectives. This detail, more often than not, requires the specification of user requirements and creation of benefits realization plans, intricately linked to the line functions that will consume the IT resources.

In the unlikely circumstance that the CIO is not the appropriate person to deal with ITG the CIO's role and responsibilities pertaining to ITG must be defined thoroughly. With the conventional definition of a CIO all but including responsibility for ITG, key to accountability is a clear segregation of duties between the person responsible for implementing ITG and the (non-responsible) CIO.

Operational management

According to Mullins and Klinowski (2003), the Chief Technology Officer (CTO) is the "right hand of the CIO" and responsible for "designing and recommending the appropriate technology solutions to support the policies and directives issued by the CIO". This approach establishes the CTO as the technology specialist and thus the appropriate role to ensure proper **IT Resource management**.

At the IT operational level the key challenge is efficiency (refer to Figure 3), in order to **deliver** direct **value** to the organisation. The CTO is responsible for ensuring that the correct IT resources, both human and technical, are deployed and utilised correctly. The concept of **performance management** is well entrenched into IT management and many of the metrics and norms used in IT operational management (systems availability, turnaround time, resource utilisation) relate to the efficient use of the existing resources. The discipline of IT Service Management (ITSM), as well as commonly used industry standards such as ITIL and CoBiT, has actually grown from the challenges pertaining to efficient IT operations and many of the frameworks used for ITG stem from within the ITSM domain.

Operational management is responsible for implementing the necessary structures, processes and mechanisms to ensure application of the ITG framework in the day-to-day activities. It is recommended that operational management increase transparency and provide the board with complete, timely, relevant, accurate and accessible information about aspects such as (IODSA, 2009; Liell-Cock, *et al*., 2009) the likelihood of IT achieving its objectives; IT's resilience to learn and adapt; the judicious management of the inherent risks arising from using IT and how well IT has recognized opportunities and acted on them.

A direct link to **risk management** exists at the operational level where management has to demonstrate that sufficient controls are in place to address IT related risks. Where the risks at tactical and strategic level mostly pertains to 'doing the rights things' to ensure that the strategic direction remains relevant, the operational risks are strongly tied into continued business operations. Continued business operations that are mostly addressed within the portfolio of business continuity (or disaster recovery) are usually well understood and overseen by organisations. However, addressing business continuity forms part of the overall concept of ITG at an operational level.

Supporting committees

Where appropriate, King (IODSA, 2009) provides for the board to appoint the necessary supporting committees to which certain responsibilities are delegated in order to ensure that the objectives of IT governance are achieved.

It is essential that IT issues are communicated between the board and management. Entities might consider establishing an IT strategy or similar committee for this purpose (Pultorak & Kerrigan, 2005). King suggests that in striving to achieve ITG the board may appoint an IT steering

committee or similar function, with relevant representation from business and IT, to assist them in the governance of IT, and that the board also be assisted by two of its subcommittees, namely the risk committee and the audit committee. CIOs are expected to attend the meetings of the audit and risk committees.

The audit committee has to consider IT as it relates to financial reporting and the going concern issues of the entity. In addition, the audit committee should consider how the use of IT and related techniques can assist the committee to improve audit coverage and audit efficiency (IODSA, 2009; Liell-Cock, *et al.*, 2009). King recommends that audit committee members' IT experience be taken into account when considering the composition of the audit committee with a view to their ITG responsibilities.

In the Code of Governance Principles King III emphasizes the principle that IT should form an integral part of an entity's risk management process. A risk management plan must be adopted by the board, which may task a risk committee to oversee **risk management** to ensure that the broader risk implications of IT are addressed adequately. The board is to determine and communicate the entity's levels of risk tolerance and ensure that key risks are identified, quantified and are responded to appropriately.

The risk committee should take the necessary steps to ensure that all IT risks are adequately addressed, including obtaining appropriate assurance on this matter. This includes aspects relating to disaster recovery as well as compliance with applicable IT-related laws, rules, codes and standards.

As the levels of IT involvement and sophistication vary from one organisation to the next, IT risk management is a fairly specialised field and organisation-specific. The risk that stems from using IT within an organisation is context-specific and where certain organisations' business processes are intertwined with technology, others are not necessarily dependent on IT to the same extent. Conversely, some types of IT-intrinsic investments are significant, yet the business benefits are extremely difficult to quantify and the business case is strongly founded within reduced risks for business operations (Benaroch, Lichtenstein & Robinson, 2006).

Summary of key responsibilities for ITG derived from King III

Table 4 contains a summary of the key responsibilities for ITG that links the respective parties mentioned in King III to the IT governance focus area that was derived when analysing the particular party's responsibilities according to King III.

Table 4: King III roles and typical responsibilities regarding ITG

Party	Responsibilities derived from King III	ITG focus area
Board	Understand IT Accept overall responsibility for IT governance Place IT on board agenda Provide appropriate leadership and direction regarding ITG Ensure that appropriate IT governance framework and processes are in place to ensure that all of the IT governance outcomes/objectives are achieved Delegate relevant responsibilities to relevant parties	Strategic alignment Performance management Value delivery Risk management IT Resource management
CEO	Appoint individual responsible for IT governance	Strategic alignment Risk management
CIO	Regularly interact with board, executive management and appropriate committee regarding ITG matters Act as bridge between business and IT Understand accountability and responsibility for IT Understand business requirement, long-term business strategy and translate into effective IT solutions Facilitate integration of IT into business Design, develop, implement and maintain sustainable IT solutions to ensure achieving strategic goals	Strategic alignment Performance management
CTO	Implement and execute appropriate IT governance framework Provide feedback to CIO/CEO Demonstrate that adequate measures for disaster recovery is in place Implement information security strategy	Value delivery Risk management IT Resource management
Risk committee	Assist board in carrying out IT responsibilities Consider entity's exposure to IT risks and ensure IT risks are adequately addressed through effective controls	Risk management
Audit committee	Assist board in carrying out IT responsibilities Responsible for IT as it relates to financial reporting and going concern Consider IT and related techniques' use to improve audit coverage and efficiency	

Conclusion

In their seminal article *Information Technology and the Board of Directors*, Nolan and McFarlan (2005) reported that "boards have grown increasingly nervous about corporate dependence on information technology". Nolan and McFarlan argued that "given the dizzying pace of change in the world of IT, boards can't afford to ignore the state of their IT systems and capabilities. Appropriate board governance can go a long way toward helping a company avoid unnecessary risk and improve its competitive position."

In Section 4 and Figure 2 in particular the authors identified the focus areas of ITG in terms of King III. These were shown to correlate to the key concepts of ITG according to leading authors (Table 3). This clearly indicates that in complying with King III South African organisations are addressing more than merely the seven ITG principles defined in the King III Report – they are addressing the key focus areas of ITG as identified by international best practices.

It is also evident from the arguments presented, and Section 4 in particular, that adherence to King III will require organisations to go beyond the principles and guidelines contained within King III and in all probability adopt a standard framework with the associated processes, structures and communication.

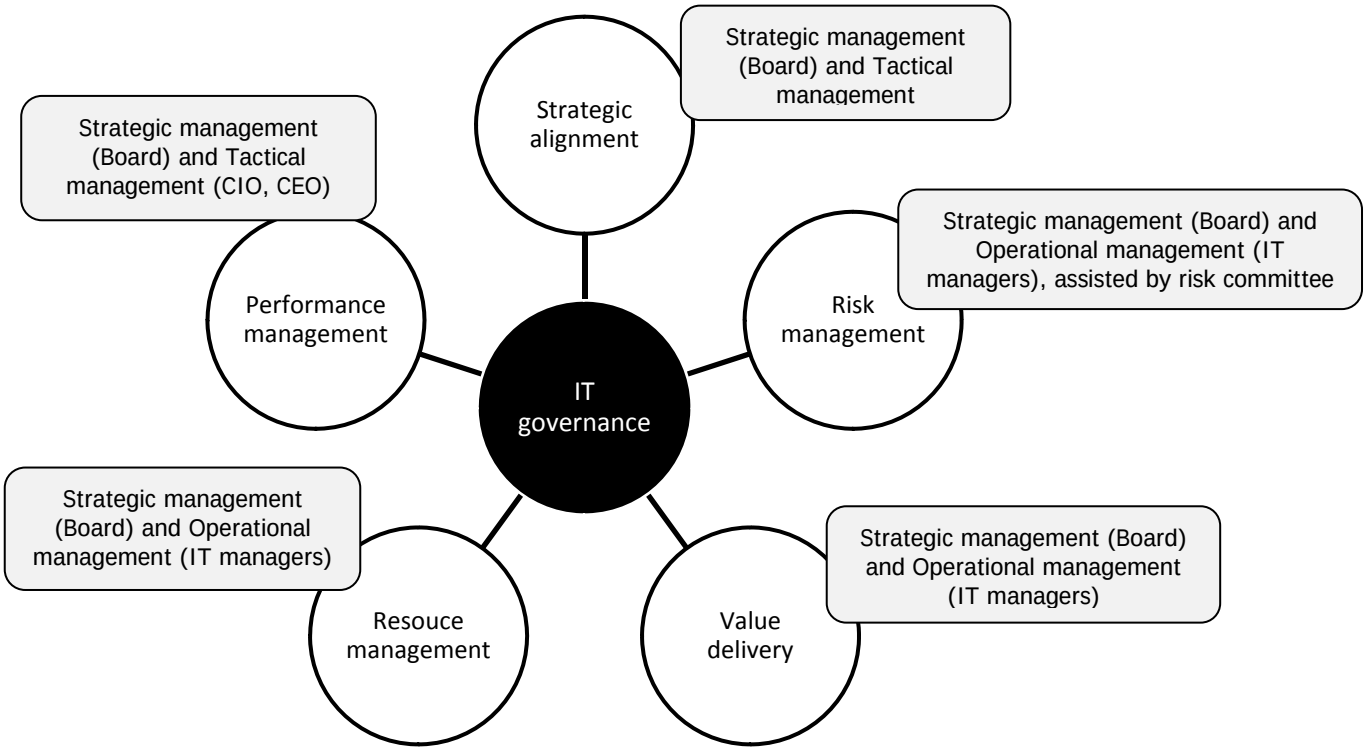

Figure 4: Management levels and ITG focus areas

Figure 4 visually depicts the focus areas for ITG and the associated management roles that should accept accountability for the ITG objectives, irrespective of the ITG framework chosen. Table 4 provides a summary of the typical management responsibilities and roles involved in ITG as derived from King III.

The King III report that mandates ITG as part of an entity's overall corporate governance effort requires compliance from all South African entities. Boards of directors and those charged with governance within South African entities need to assume their new roles and responsibilities with regard to ITG. This study defined and analysed the macrolevel objectives of ITG for South African entities that have to apply King III, by formulating five focus areas (Figure 2). These focus areas were shown to correlate to key literature, and hence provide a comprehensive macrolevel view of ITG (Table 3). These focus areas can serve as a solid point of departure to introduce ITG conceptually at board level

It is important to note that the responsibility to achieve ITG does not necessarily mean that all entities will have to start from a zero base. The majority of entities who have to apply King III principles already have some degree of IT control in place, albeit on an ad hoc and informal basis, or formally embedded within the entity's wider governance structures.

Entities with informal processes will have to formalize their governance process to adhere to King III, similarly to the process that followed after the introduction of the Sarbanes Oxley Act in the USA in 2002, when boards and executive managements were required to focus more extensively on compliance and risk management, including IT. Many South African entities may be able to customize their existing IT

control practices in the process of achieving IT Governance as required by King III.

For organisations already using a formal framework and with the correct processes, structures and communications in place, the research concludes that the definition of ITG according to King III does not extend beyond the current body of knowledge, as should be expected. In essence, King III's coverage of ITG provides an excellent set of principles that can be used to evaluate current practices within organisations.

Irrespective of where an entity finds itself with respect to ITG, accountability for a concept as significant as ITG, that is fairly poorly understood, and that cuts across all levels of management, is imperative to ensure that the *right things* are *done right*.

References

Benaroch, M., Lichtenstein, Y. & Robinson, K. 2006. 'Real options in information technology Risk management: An empirical validation of risk-option relationships', *MIS Quarterly*, **30**(4): 827–864.

Brisebois, R., Boyd, G. & Shadid, Z. 2010. 'What is IT governance?'. INTOSAI Working Group on IT Audit – IntoIT articles. [online] URL:http://*www.intosaiitaudit.org/intoit_articles/ 25_p30top35. Accessed 12 February 2010.*

Brown, A.E. & Grant, G.G. 2005. 'Framing the Frameworks: A Review of IT Governance Research', *Communications of the Association for Information Systems*, **15**: 696–712.

Buckby, S., Best, P. & Stewart, J. 2005. 'The role of boards in reviewing Information Technology Governance (ITG) as part of organizational control environment assessments'. *Proceedings 2005 IT Governance International Conference*, Auckland, New Zealand: ITGI.

Calder, A. 2008. 'Developing an IT Governance Framework'. *ITadviser,* **56**. [online] URL: http://principia.vbnlive.com/pooled/articles/BF_WEBART/view.asp,que=BF_WEBART_308733. Accessed 23 October 2009.

Canadian Institute of Chartered Accountants (CICA). 2004. '20 questions directors should ask about IT'. April. [online] URL:http://www.cica.ca. Accessed 20 October 2009.

Chun, M.W.S. 2005. 'IT matters: The IT Governance Road Map. *Graziadio Business Report,* **11**(3). [online] URL:http://www.gbr.pepperdine.edu/053/itmatters.html. Accessed 16 February 2010.

Damianides, M. 2005. 'Sarbanes-Oxley and IT governance: New guidance on IT control and compliance'. *Information Systems Management,* **22**(1): 77–85. [online] URL:http://web.ebscohost.com.ez.sun.ac.za/ehost/pdf?vid=2&hid=105&sid=795dcfce-9122-4f32-98f0-d9d369fbdd33%40sessionmgr104. Accessed 20 October 2009.

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 for Information Systems*, **22**: 443–458.

Disterer, G. 2009. 'ISO 20000 for IT', *Business & Information Systems Engineering*, **1**(6).

Drucker, P. 1977. *An introductory view of management.* New York: Harper College Press.

Griffin, R.W. 1987. *Management.* 2nd Edition. Boston: Houghton Mifflin Co.

Hardy, G. 2003. 'Coordinating IT governance – A new role for IT strategy committees', *Information Systems and Control Journal*, **4**.

IT Governance Institute (ITGI). 2003. 'Board briefing on IT governance'. [online] URL: http://www.itgi.org. Accessed 23 September 2009.

IT Governance Institute (ITGI). 2008. 'IT Governance Global Status Report 2008'. [online] URL:http://www.itgi.org. Accessed 19 October 2009.

IT Governance Institute (ITGI). 2009a. 'An executive view of IT governance'. [online] URL: http://www.itgi.org. Accessed 19 October 2009.

IT Governance Institute (ITGI). 2009b. 'ITGI enables ISO/IEC 38500:2008 adoption'. [online] URL: http://www.itgi.org. Accessed 23 October 2009.

Jordan, E.J. & Musson, D. 2004. 'Corporate governance and IT governance: Exploring the board's perspective'. 2 December. [online] URL:http://papers.ssrn.com. Accessed 23 September 2009.

Kao, C., Chen, L., Wang, T., Kuo, S. & Horng, S. 1995. 'Productivity improvement: Efficiency approach vs effectiveness approach', *International Journal of Management Science*, **23**(2): 197–204.

Institute of Directors Southern Africa (IODSA). 2009. 'King Report on corporate governance for South Africa (King III)'. [online] URL:http://www.iodsa.co.za. Accessed 23 September 2009.

Kordel, L. 2004. 'IT governance hands-on: Using CobiT to implement IT governance', *Information Systems Control Journal*, **2**.

Larsen, M.H., Pedersen, M.K., & Andersen, K.V. 2006. 'IT governance: Reviewing 17 IT governance tools and analyzing the case of Novozymes A/S'. **In** *Proceedings of the 39th Hawaii International Conference on System Science*. Kauai, Hawaii. 4-7 January 2006.

Leong, C. 1991. 'Accountability and project management: A convergence of objectives', *International Journal of Project Management*, **9**(4): 240–249.

Liell-Cock, S., Graham, J. & Hill, P. 2009. 'IT governance aligned to King III: Executive overview'. 7 September. [online] URL:http://www.itgovernance.com. Accessed 23 September 2009.

Luo, A. 2005. 'Corporate governance and accountability in multinational enterprises: Concepts and agenda', *Journal of International Management*, **11**: 1–18.

Mouzas, S. 2006. 'Efficiency versus effectiveness in business networks', *Journal of Business Research*, **59**: 1124–1132.

Mullins, S.P. & Klinowski, J.R. 2003. 'Defining the complementary job roles of the CTO and CIO'. *TechRepublic*, 18 April. [online] URL:http://articles.techrepublic.com.com/5100-10878_11-5034729 html. Accessed 12 February 2010.

Nolan, R. & McFarlan, F.W. 2005. 'Information technology and the board of directors', *Harvard Business Review*, **83**(10): 96-106.

Pultorak, D. & Kerrigan, J. 2005. 'Conformance, performance and rapport: A framework for corporate and IT governance', *Directors Monthly*, February. [online] URL:www nacdonline.org. Accessed 22 February 2010.

Raghupathi, W. 2007. 'Corporate governance of IT: A framework for development', *Communications of the ACM*, **50**(8): 94-99.

Symons, C. 2005. 'IT governance framework – Structures, processes and communication', *Forrester Research Inc*, 25 March.

Tarantino, A.G. 2008. *Governance, risk and compliance handbook: Technology, finance, environmental and international guidance – best practices*. New Jersey: John Wiley & Sons.

Trites, G. 2004. 'Director responsibility for IT Governance', *International Journal of Accounting Information Systems*, **5**: 89–99.

Weill, P. & Ross, J. 2004. W. 'Ten principles of IT governance'. Harvard Business School Working Knowledge. [online] URL:http://hbswk.hbs.edu/archive/4241 html. Accessed 8 February 2010.