

Mapping the Information Technology (IT)  
governance requirements contained in the King  
III Report to the IT domains and processes of  
the Control Objectives for Information and  
Related Technology (COBIT) framework

by  
Gretha Steenkamp

*Thesis presented in partial fulfilment of the requirements for the degree  
Master of Accounting (Computer Auditing) at the University of*

*Stellenbosch*



Supervisor: Prof Willie Boshoff  
Co-supervisor: Prof Rika Butler  
Faculty of Economic and Management Sciences  
Department of Accounting

December 2009

# Mapping the Information Technology (IT) governance requirements contained in the King III Report to the IT domains and processes of the Control Objectives for Information and Related Technology (COBIT) framework

## RESEARCH ARTICLE:

**MAcc (Computer Auditing): Gretha Steenkamp (13165046)**

### **Abstract:**

Due to the integration of IT into all aspects of modern-day businesses, it is vital that the risks associated with IT are governed as an integral element of enterprise-wide corporate governance. The Third King Report on Corporate Governance (King III) was issued by the South African Chapter of the Institute of Directors in September 2009 and becomes operational on 1 March 2010. This marks the first time that the King Report has specifically addressed IT governance.

King III will apply to all corporate entities. Such entities could benefit from applying an IT governance framework to ensure that they adequately address all aspects of IT governance, as required by King III. One of the comprehensive frameworks available is COBIT (Control Objectives for Information and Related Technology) issued by ISACA (previously known as the Information Systems Audit and Control Association). King III mentions the fact that COBIT could be used to assess and implement IT governance within an entity.

The aim of this research is to determine whether the use of COBIT ensures compliance with King III's requirements relating to IT governance. It was found that the main requirements in King III relating to IT governance and the processes of COBIT are well aligned, and, as a result, COBIT could be used effectively to ensure compliance with King III in relation to IT governance. However, an entity would still have to pay attention to certain King III-specific requirements.

Furthermore, it was found that the application of the principles in COBIT could further strengthen the IT governance of an entity, as COBIT also addresses the more detailed activities, such as the implementation and operation of the IT system, which is not specifically addressed by King III.

## **OUTLINE OF SECTIONS**

	<b>Page</b>
1. Introduction	1
2. Research methodology	3
3. IT governance	4
3.1 Introduction to IT governance	4
3.2 The benefits of IT governance	5
3.3 The responsibility for IT governance	5
3.4 The use of IT governance frameworks	6
4. COBIT as an IT governance framework	8
5. The results of mapping King III and COBIT	9
5.1 Aspects contained in COBIT, but not addressed by King III	11
5.2 New principles introduced by King III	12
6. Conclusion	15
7. References	16

## **1. INTRODUCTION**

Modern-day organisations rely heavily on their Information Technology (IT) systems and would, in many instances, not be able to achieve their business goals effectively without them. IT is also used to store and manage the financial and other data of the entity, for internal and external reporting purposes (Etzler, 2007 and De Goede, 2003).

According to IBM (2006) and COBIT 4.1 (2007), many entities are increasing their investment in IT-related assets. Many IT systems rely on complex technologies and are therefore embedded into the entity's operations (Hardy, 2006 and Peterson, 2004). According to King III (2009), "Information systems were used as an enabler of business, but have now become pervasive in the sense that they are built into the strategy of the business. The pervasiveness of IT in business mandates the governance of IT as a corporate imperative".

The use of IT in this manner holds many advantages, but also exposes an entity to additional risks (De Goede, 2003). According to Hardy (2006), Vecchiatto (2009) and King III (2009), these risks include:

- unauthorised use of and access to the IT system and information,
- unauthorised changes to the IT system,
- compromising confidential information,
- loss of income due to disruption and poor functioning of the IT system, and
- possible legal action against the entity.

It is vital that the risks associated with IT, IT-related assets and IT-related information are assessed, just as with any other major risk of an entity (Hardy, 2006). Internal control processes should be put in place to mitigate the identified risks surrounding IT. The assessment of risks and the mitigation of these risks through controls, as mentioned in the previous paragraph, form a part of corporate governance. Corporate governance is the system by which an entity is "directed and controlled" (Van Grembergen, 2004) by the entity's board of directors and management (Kose & Lemma, 1998). Due to the integration of IT into all aspects of business, IT governance is an integral part of effective corporate governance (Von Solms & Von Solms, 2005 and De Goede, 2003).

For South African entities, one of the most important guidelines on what constitutes good corporate governance is the King Report issued by the South African Institute of Directors. The King Report strives to provide guidelines and principles relating to the best practices for corporate governance in the South African context (Buys, 2009). The Third King Report on Corporate Governance (King III) was released in September 2009. This marks the first time that the King Report has specifically addressed IT governance.

King III becomes operational on 1 March 2010 and will apply to all corporate entities, regardless of their size and whether they are listed or not. The previous King reports (King I and II) were only applicable to listed entities. This makes it all the more critical for all entities in South Africa to grasp the implications of King III for IT governance, and to understand what they can do to meet these requirements (Buys, 2009).

King III does not provide a specific set of rules applicable to all entities (Buys, 2009), rather it is a “principle-based document” (Temkin, 2009). Therefore, it is necessary for the management of each company to understand the principles contained in King III and then apply these principles to their company’s specific situation. King III (2009) stated that the use of an IT governance framework during this process could be beneficial. One of the comprehensive frameworks available is COBIT (Control Objectives for Information and Related Technology) issued by ISACA (previously known as the Information Systems Audit and Control Association). King III makes mention of the fact that COBIT can be used to assess and implement IT governance, although it does not state how.

The aim of this research is to determine whether COBIT can be used to achieve compliance with King III’s requirements relating to IT governance. In achieving this goal, the requirements in King III relating to IT governance were summarised and then mapped to COBIT (as a framework for IT governance). Those responsible for corporate governance within an entity will benefit from this research as it will help them gain a concise understanding of the requirements of King III relating to IT governance, as well as how they could employ COBIT in achieving compliance with those requirements.

## **2. RESEARCH METHODOLOGY**

In order to create a concise summary of King III's requirements relating to IT governance and then compare them to COBIT, the following methodology was followed:

Firstly, a literature review was conducted on all aspects involved, namely (i) the King Report, specifically King III; (ii) the need for IT governance; (iii) what IT governance entails; (iv) COBIT and (v) any existing mapping of COBIT and the King Report.

Secondly, a detailed study was made of King III. All aspects that either directly or indirectly address the area of IT governance were tabled. This comprehensive list of the IT governance requirements contained in King III was then condensed into the main requirements.

Thirdly, the IT domains and processes of COBIT were studied, and then linked to the condensed main requirements of King III (as described above). This allowed requirements regarding IT governance contained in both documents to be mapped. This mapping demonstrates how COBIT can be used as a tool in achieving compliance with King III.

Lastly, all aspects relating to IT governance not addressed by both King III and COBIT were pinpointed. Those aspects contained in King III, but not in COBIT, were assessed to ascertain how they impact the effectiveness of using COBIT as a tool in achieving compliance with King III. Those aspects addressed by COBIT, but not King III, were assessed to ascertain why King III does not address them and whether they are also valid aspects that should be included in an entity's process of governing IT.

### **3. IT GOVERNANCE**

#### **3.1 Introduction to IT governance**

According to Van Grembergen (as cited by Etzler, 2007), "IT governance is the organisational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT". IT governance includes (i) understanding the risks surrounding IT, (ii) managing those risks through IT security and other controls, (iii) the strategic alignment of business and IT (ensuring that IT supports the business goals and direction) and (iv) the management of IT resources (Hardy, 2006 and King III, 2009).

According to King III (2009), "In IT governance one seeks confidentiality; integrity and availability of the functioning system; possession of the system; authenticity of system information; and assurance that the system is usable and useful". IT governance comprises the people ("Who") and procedures ("How") through which an entity manages its IT resources, rather than the specific "what needs to be done" (Peterson, 2004).

The optimal IT governance approach for a specific entity depends on various factors, such as the entity's industry, financial situation, existing IT management processes as well as the level of usage, complexity and integration of IT in the business (Nolan & McFarlan, 2005). IT governance is not a once-off development of an internal system, but rather a continuous process by which management regularly assesses the emerging risks of new applications, technologies and business models (Williams, 2007) and then tries to address these risks.

Every company has an IT governance model, even though it may never have been formalised. If it has been formally documented, the reality might be that the written and applied models of IT governance differ. It is therefore important that IT governance practices are monitored against a pre-determined ideal (Peterson, 2004).

The governance of IT is driven primarily by the need to comply with external regulations (such as King III), although most entities do recognise the benefits of good governance because it "truly can contribute to the overall cost efficiency and performance of IT" (Etzler, 2007).

### 3.2 The benefits of IT governance

Entities with effective IT governance processes are likely to experience the following benefits (Bowen, Cheung & Rohde, 2007; Hardy, 2006; Spafford, 2003; De Haes & Van Grembergen, 2008 and IBM, 2006):

- the reputation of the entity is improved;
- trust is built within the entity as well as externally;
- risks in general are diminished (and specifically the risk of financial damage and legal action due to an IT malfunction or malicious attack on the IT system); and
- the strategic alignment of IT with business goals and processes is achieved, leading to a competitive advantage (through decreased costs, increased customer satisfaction and the ability to respond to business opportunities and challenges faster) which ultimately leads to an increase in revenue.

### 3.3 The responsibility for IT governance

King III places the onus of IT governance firmly on the shoulders of the board of directors of a company. Mr Mervyn King, head of the committee that compiled the King Report, stated the following, “A company’s board must be directly involved in IT governance” (Vecchiato, 2009) by ensuring that IT governance is addressed adequately (King III, 2009). IT governance is reported to be most effective if it is frequently discussed by the board (Hardy, 2006).

COBIT 4.1 (2007) also emphasises that IT governance should be addressed by the top management and the board of directors of a specific entity. As per section 424 of the Companies Act 61 of 1973, as amended, a director or manager may be personally liable if their failure to assess and address IT risks is seen as reckless management of the company (Von Solms & Von Solms, 2005).



### 3.4 The use of IT governance frameworks

King III lays down guidelines for good IT governance. It also acknowledges that there is no 'one-size-fits-all' set of rules for IT governance for all organisations, as they differ in size, level of use of IT and integration of IT into business (King III, 2009).

However, it is important that an entity develops, implements and maintains a formal, understandable and measurable strategy for IT governance. An entity can either develop such a strategy independently or use an existing internationally accepted framework on IT governance – such as COBIT, ITIL (Information Technology Infrastructure Library) or ISO 17799 (the International Organisation for Standardisation's ISO 17799, titled "Information Technology – Code of Practice for Information Security Management") (Hardy, 2006).

King III (2009) mentions that the use of an IT governance framework could aid the implementation of IT governance within a specific entity (especially when attempting to comply with the requirements of King III). The benefits of this are as follows:

- A decrease in the costs involved (Etzler, 2007) as the development is structured (Spafford, 2003) and therefore shorter;
- The effectiveness of the end product is enhanced (Etzler, 2007) as frameworks are best practices developed by many participants (Spafford, 2003), ensuring that all aspects are covered; and
- It allows for easy assessment to prove compliance with external regulations (Spafford, 2003).

The usefulness of applying an IT governance framework when developing internal IT governance practices (that need to comply with external regulations), is evident when one considers a situation similar to that of South African entities and King III. In the United States of America (USA) entities have to comply with the requirements of the Sarbanes-Oxley Act (SOX). SOX was issued by the Congress of USA in 2002 to provide guidance on and requirements for corporate governance for USA entities. SOX, similarly to King III, offers broad-based principles, rather than detailed procedures, and leaves the implementation of these principles up to the entity itself. In research conducted by Haworth & Pietron (2006) it was argued that entities applying the principles in ISO 17799 as IT governance framework have complied with the requirements of SOX in many respects.

In conducting this research, COBIT was singled out from the available IT governance frameworks. The motivation for this can be summarised as follows:

- COBIT is mentioned in King III as one of the possible IT governance frameworks to apply in achieving IT governance,
- COBIT is a comprehensive framework, covering all the important elements of IT governance, rather than focussing on a specific part of it, as ISO 17799 and ITIL do,
- It is business-orientated,
- It is internationally accepted,
- It is available free of charge,
- COBIT incorporates the consensus of experts,
- It can be used by any organisation towards IT governance – as it can be adapted to the size, level of IT usage, complexity and needs of each different organisation, and
- COBIT is often used by managers and auditors to assess an entity's system of IT internal control for compliance with SOX (a similar scenario to the one studied in this research).

(King III, 2009; Spafford, 2003; Simonsson & Johnson, 2006; Williams, 2006; De Goede, 2003; Grant, Miller & Alali, 2008; Etzler, 2007; Bowen, Cheung & Rohde, 2007 and COBIT 4.1, 2007)

For these reasons COBIT, rather than any other IT governance framework, was chosen as the framework to which King III's requirements relating to IT governance will be compared during this research.

## **4. COBIT AS AN IT GOVERNANCE FRAMEWORK**

COBIT is an IT governance framework or set of best practices for IT governance. The mission of COBIT is: “To research, develop, publicise and promote an authoritative, up-to-date, internationally accepted IT governance control framework for adoption by enterprises and day-to-day use by business managers, IT professionals and assurance professionals.” (COBIT 4.1, 2007)

COBIT can be applied to identify IT-related business risks, the IT issues surrounding these risks and identify control measures that should be put in place (Williams, 2006). It provides a logical structure through which an entity can develop and implement a system of IT governance that is suitable for its operations and addresses its individual risks (COBIT 4.1, 2007).

The COBIT framework is structured into four domains which constitute the primary “responsibility” areas or aspects which an IT governance framework should address to ensure effective functioning on all levels. These domains are similar to the IT functions of “plan, build, run and monitor”. Each of the domains mentioned above is then divided into further subcategories, detailing specific processes which must take place to ensure IT control. (COBIT 4.1, 2007)

The four domains mentioned in COBIT, according to COBIT 4.1 (2007), are:

- Plan and Organise (PO) describes how IT strategy should be developed to align with the business goals.
- Acquire and Implement (AI) describes the identification, acquisition and implementation of IT solutions (hardware and software) as well as the management of changes to existing systems.
- Deliver and Support (DS) describes the day-to-day operation of the IT system and how this should be managed. The operations include, among others, the management of service levels; performance and capacity; configurations, operations and the physical environment; allocation of costs and the training of users.
- Monitor and Evaluate (ME) describes the monitoring and evaluation of IT performance, IT controls and external compliance. It also states that an entity should “provide IT governance”.

## **5. THE RESULTS OF MAPPING KING III AND COBIT**

After tabling all the requirements in King III that relate to IT governance, a summary of these requirements was made, grouping similar items together (see column one in Table 1 below for the summary). Eight main requirements were identified. These main requirements were then linked to the domains and processes (columns two and three of Table 1 below) of COBIT (as these form the mainstay and logical structure of COBIT).

**TABLE 1**

<b>Main requirements relating to IT governance in King III</b>		<b>Links to relevant COBIT domains</b>	<b>Links to relevant COBIT processes</b>
<b>1</b>	<b>IT governance should take place</b>	Monitor and Evaluate	ME4 - Provide IT governance
<b>2</b>	<b>Board (and management) responsibility</b>	Plan and Organise	PO1 - Define a strategic plan PO3 - Determine technological direction
	(i) Use of risk committee, audit committee and IT steering committee to monitor/govern	Plan and Organise Monitor and Evaluate	PO1 - Define a strategic plan PO3 - Determine technological direction ME1 - Monitor and evaluate IT performance ME2 - Monitor and evaluate internal control
	(ii) Communication inside entity	Plan and Organise	PO6 - Communicate management aims and direction
	(iii) Appoint CIO as bridge between business and IT	Plan and Organise	PO7 - Manage IT human resources
<b>3</b>	<b>Alignment of business with IT</b>	Plan and Organise	PO1 - Define a strategic plan PO3 - Determine technological direction
<b>4</b>	<b>Assess IT risks</b>	Plan and Organise	PO9 - Assess and manage IT risks
	(i) With outside service provider	Deliver and Support	DS2 - Manage third-party services

Main requirements relating to IT governance in King III	Links to relevant COBIT domains	Links to relevant COBIT processes
5 <b>Manage IT risks by ensuring IT and information security and privacy (through IT controls and other measures)</b>	Plan and Organise Deliver and Support Monitor and Evaluate	PO9 - Assess and manage IT risks DS5 - Ensure systems security ME2 - Monitor and evaluate internal control
(i) Safeguarding of IT assets (especially information)	Plan and Organise Deliver and Support	PO9 - Assess and manage IT risks DS5 - Ensure systems security DS11 - Manage data DS12 - Manage the physical environment
(ii) Business continuity/Disaster recovery	Deliver and Support	DS4 - Ensure continuous service
6 <b>Management of:</b>	Plan and Organise Acquire and Implement Deliver and Support	PO7 - Manage IT human resources AI5 - Procure IT resources DS1-13 (entire Deliver and Support)
(i) <b>PEOPLE</b> (Corporate structure/ Human resources should support IT strategy)	Plan and Organise	PO7 - Manage IT human resources
(ii) <b>FUNDING</b> (Value delivery of IT, optimising expenditure)	Deliver and Support Plan and Organise Monitor and Evaluate	DS6 - Identify and allocate costs PO5 - Manage the IT investment ME1 - Monitor and evaluate IT performance
(iii) <b>INFORMATION &amp; IT SYSTEM</b>	Deliver and Support	DS1-13 (entire Deliver and Support)
(iv) <b>CHANGE</b> (Management of changes to information system, processes and functioning of personnel)	Acquire and Implement Deliver and Support	AI6 - Manage changes DS7 - Educate and train users
(v) <b>IT PROJECTS</b> (project management)	Plan and Organise	PO10 - Manage projects
7 <b>Monitoring of IT performance, IT governance and the effectiveness of IT security/IT controls (could use internal audit function)</b>	Monitor and Evaluate Plan and Organise	ME1 - Monitor and evaluate IT performance ME2 - Monitor and evaluate internal control PO8 - Manage quality
8 <b>Compliance with external requirements and laws</b>	Monitor and Evaluate	ME3 - Ensure compliance with external requirements

## 5.1 Aspects contained in COBIT, but not addressed by King III

From table 1 it is evident that the “Plan and Organise” and “Monitor and Evaluate” domains of COBIT were addressed comprehensively by King III. However, the more practical processes of COBIT (contained in the domains “Acquire and Implement” and “Deliver and Support”), such as the operation of the hardware and software, as well as the management of the day-to-day activities, were not addressed by King III. The reason for this is that King III is not prescriptive, nor does it aim to comprehensively address all IT governance issues. It is in these areas that COBIT can be most helpful in providing additional guidelines towards the attainment of good IT governance.

The following is a list of the aspects contained in COBIT but not addressed by King III:

- (i) COBIT requires that IT governance policies be documented (COBIT 4.1, 2007), but King III does not explicitly require any such evidence. King III (2009) does, however, require the documentation of the risk management policy and plan (which should include the IT risk management policies and plans) as well as the documentation of the ISMS (information security management system).
- (ii) “PO8 – Manage Quality” is a process of COBIT that entails the establishment of a Quality Management System – i.e. an instrument by which IT performance may be measured (COBIT 4.1, 2007). King III does not explicitly mention the monitoring of IT performance. It requires the monitoring of material IT investments and expenditure, but it does not specifically state how they should be measured. “PO8 – Manage Quality” can be of great service in this regard.
- (iii) The “Acquire and Implement” domain of COBIT deals mainly with the practical issues surrounding the selection of an appropriate hardware and software solution to enable the entity’s IT strategy, as well as the implementation of the IT (COBIT 4.1, 2007). No mention is made of this aspect in King III, except to state that changes to the system should be monitored (King III, 2009). These processes in COBIT could be used to give structure to the IT projects within an entity, providing guidance on how to choose the best IT applications, install them and ensure that they operate correctly.

- (iv) The “Deliver and Support” domain contains the processes that COBIT employs to ensure optimal and effective operation of the IT system on a day-to-day basis, such as defining how the IT system should operate (based on the needs of the users); ensuring that it does operate according to these requirements; managing the service desk, incidents and problems; training users and managing the configuration (COBIT 4.1, 2007).

Very little mention is made of these day-to-day aspects of IT governance in King III, as it aims to be more broad-based, and provides guidance on a higher level. However, the processes contained in the “Deliver and Support” domain can help an entity to manage their IT operations on a day-to-day basis and thereby reduce the so-called “IT gap” (the gap between what IT operations and personnel actually do and what is expected from IT by management).

The requirement that IT resources be managed (see requirement six in Table 1 in section 5) links to the “Deliver and Support” domain, although very little is stated about the practical attainment of this goal in King III.

## 5.2 New principles introduced by King III

King III introduced a number of IT governance ideas or concepts that are not covered by COBIT, as can be seen in A to E below. COBIT does not address these aspects, because COBIT provides a high level framework of what should be done in terms of governance rather than stipulating exactly how each company should achieve this (Etzler, 2007). The aspects mentioned below focus mainly on the establishment of internal committees of directors and other internal functions, which will aid the IT governance process. COBIT does not address these aspects as this would be too prescriptive for a framework seeking to provide general, widely-applicable guidelines.

### A – The board is responsible for IT governance

King III (2009) states (in principle 5.1) that the board of directors should be responsible for IT governance (the development, implementation, maintenance and monitoring of an internal IT governance process), ensuring that all IT risks are assessed and mitigated through IT controls and information security.

COBIT 4.1 (2007) also states that IT governance should take place, but does not prescribe how this should be achieved and by whom.

### B – The use of an audit and/or risk committee

As per principle 5.7 in King III (2009), a risk committee and/or audit committee should be tasked with IT governance, to assist the board of directors in this regard. The use of a committee to assist the directors with IT governance leads to improved project management and cost management of IT projects and enables the alignment of IT and business in reaching enterprise goals (Nolan & McFarlan, 2005).

The risk committee should ensure that all IT risks are assessed and managed by means of controls, and that the effectiveness of this process is monitored. The audit committee is responsible for assessing the impact of IT on a going concern and on financial reporting. It should also oversee the internal audit function, integrated reporting and play a pivotal role in risk management activities. (King III, 2009)

Again, COBIT does state that the processes mentioned above should take place, but does not prescribe how this should be achieved and by whom.



### C – Appointment of a CIO (Chief Information Officer)

Another new development in King III is the mandating of the role of the CIO – an individual charged with the management of the IT function – who should be experienced and educated in matters relating to business and IT. The CIO should also be able to communicate effectively regarding IT matters with the board of directors as well as management. (King III, 2009)

King III (2009) advises that the role of the CIO is to diminish the misalignment between business needs and IT operations, enabling the IT function to support business activities. The CIO should be knowledgeable regarding IT governance, IT's everyday functioning as well as the business objectives and strategies of the company – so as to ensure that these aspects are aligned (IBM, 2006).

### D – Employ internal audit team (reports to audit committee)

King III (2009) advises that a risk-based internal audit is conducted to evaluate IT risks, IT management and IT governance in particular. COBIT 4.1 (2007) does not explicitly sanction the use of an internal audit function, but it does require IT risks and controls to be assessed and monitored. King III has provided an effective way to achieve this goal.

### E – Green IT and sustainability

King III requires entities to consider the use of green IT principles and focus on the sustainability of IT and operations during the strategic alignment of business and IT.

## **6. CONCLUSION**

According to Hardy (2006) the effective governance of IT is a distinguishing factor in the eventual success of an entity. If an entity employs IT in the attainment of its business goals and its everyday operations, it has to make provision for adequate controls to mitigate the accompanying additional risk exposure.

Recently there has been an increased focus on the regulation of entities internationally and also in South Africa. The Third King Report (King III), which was issued in September 2009 and becomes operational on 1 March 2010, placed increased emphasis on corporate governance by laying down fundamental principles for good corporate governance by South African entities.

King III will apply to all corporate entities and has, for the first time, given specific guidance regarding IT governance in a separate chapter of the report. King III mentioned that entities could benefit from employing an IT governance framework when developing, implementing and monitoring internal IT governance, as required by King III. One of the prominent IT governance frameworks available is COBIT, which was used in this research.

This research analysed the requirements of King III relating to IT governance and summarised them in Table 1. King III's requirements relating to IT governance were then mapped to the IT domains and processes of COBIT. When compared to the domains and processes of COBIT, it was found that the IT governance requirements contained in King III are valuable, but that they focus mainly on the broader aspects of governance, such as the planning and monitoring that must be done by the directors. King III does not address the more detailed activities, such as the implementation and operation of the IT system.

In conclusion, it was found that the requirements in King III relating to IT governance and the processes of COBIT are well aligned, and, as a result, COBIT could be used effectively to ensure compliance with King III in the creation of an internal IT governance framework for an entity. However, an entity would still have to pay attention to certain King III-specific requirements, such as the responsibilities of the board of directors, audit committee, risk committee and CIO.

## **7. REFERENCES**

- Bowen, P.L., Cheung, M.D. & Rohde, F.H. 2007. Enhancing IT governance practices: A model and case study of an organization's efforts. *International Journal of Accounting Information systems*, 8:191-221.
- Buys, R. 2009. *IT Governance Report slated*. [Online]. Available: <http://mybroadband.co.za/news/General/7242.html> (Accessed 10 July 2009).
- COBIT 4.1. 2007. IT Governance Institute 2007. [Online]. Available: <http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981> (Accessed 10 July 2009).
- De Goede, S. 2003. *Application of COSO to manage information technology in terms of the King II report requirements*. Unpublished master's thesis. Stellenbosch: University of Stellenbosch.
- De Haes, S. & Van Grembergen, W. 2008. Analysing the Relationship between IT Governance and Business/IT Alignment Maturity. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), 2008*. [Online]. Available: <http://www2.computer.org/portal/web/csdl/doi/10.1109/HICSS.2008.66> (Accessed 5 October 2009).
- Etzler, J. 2007. *IT GOVERNANCE ACCORDING TO COBIT: How does the IT performance within one of the largest investment banks in the world compare to COBIT?* [Online]. Available: [http://www.ee.kth.se/php/modules/publications/reports/2007/XR-EE-ICS\\_2007\\_014.pdf](http://www.ee.kth.se/php/modules/publications/reports/2007/XR-EE-ICS_2007_014.pdf) (Accessed 10 July 2009).
- Grant, G.H., Miller, K.C. & Alali, F. 2008. The effect of IT controls on financial reporting. *Managerial Auditing Journal*, 23(8):803 – 823.
- Hardy, G. 2006. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security Technical Report II*: 55-61.

Haworth, D.A. & Pietron, L.R. 2006. *Sarbanes-Oxley: Achieving compliance by starting with ISO 17799*. [Online]. Available: <http://www.ism-journal.com/ITToday/SOX.pdf> (Accessed 15 July 2009).

IBM. 2006. Igniting *innovation through business and IT fusion*. [Online]. Available: [http://www-935.ibm.com/services/fr/cio/flexible/flex\\_wp\\_gts\\_fusion\\_business\\_it.pdf](http://www-935.ibm.com/services/fr/cio/flexible/flex_wp_gts_fusion_business_it.pdf) (Accessed 10 July 2009).

King III Report. 2009. [Online]. Available: <http://african.ipapercms.dk/IOD/KINGIII/kingiiiireport> (Accessed 5 October 2009).

Kose, J. & Lemma W. S. 1998. Corporate governance and board effectiveness. *Journal of Banking & Finance*, 22(4): 371-403.

Nolan, R. & McFarlan, F.W. 2005. Information Technology and the Board of Directors. *Harvard Business Review*, 83(10):96-106.

Peterson, R. 2004. Crafting information technology governance. *EDPACS*, 32(6):1-23.

Simonsson, M. & Johnson, P. 2006. Assessment of IT Governance – A Prioritization of Cobit. *Proceedings of The Conference on Systems Engineering: Paper #151*. [Online]. Available: [http://www.ee.kth.se/php/modules/publications/reports/2006/IR-EE-ICS\\_2006\\_007.pdf](http://www.ee.kth.se/php/modules/publications/reports/2006/IR-EE-ICS_2006_007.pdf) (Accessed 10 July 2009).

Spafford, G. 2003. *The Benefits of Standard IT Governance Frameworks*. [Online]. Available: <http://www.itsmwatch.com/itil/article.php/2195051> (Accessed 15 July 2009).

Temkin, S. 2009. *King 3's IT governance provisions under fire*. [Online] Available: <http://www.fmtech.co.za/?p=10963> (Accessed 9 July 2009).

Van Grembergen, W. 2004. *Strategies for information technology governance*. London: Idea Group Publishing.

Vecchiato, P. 2009. *King III addresses IT governance*. [Online]. Available: <http://www.itweb.co.za/sections/business/2009/0902261041.asp?S=Legal%20View&A=LEG&O=FPLEAD> (Accessed 9 July 2009).

Von Solms, B. & Von Solms, R. 2005. From information security to ... business security? *Computers & Security*, 24: 271-273.

Williams, P. 2006. *A helping hand with IT governance*. [Online]. Available: <http://www.computerweekly.com/Articles/2006/09/19/218517/a-helping-hand-with-it-governance.htm> (Accessed 10 July 2009).

Williams, P. 2007. Executive and board roles in information security. *Network Security*, 2007(8):11-14.