# AN ANALYSIS OF COBIT 5 AS A FRAMEWORK FOR THE IMPLEMENTATION OF IT GOVERNANCE WITH REFERENCE TO KING III

L Maseko*, B Marx*

*Department of Accountancy, University of Johannesburg, South Africa

## Abstract

Owing to the complexity and general lack of understanding of information technology ("IT"), the management of IT is often treated as a separately managed value-providing asset. This has resulted in IT rarely receiving the necessary attention of the board, thus creating a disconnect between the board and IT. The King Code of Governance for South Africa 2009 (hereafter referred to as "King III") provides principles and recommended practices for effective IT governance in order to create a greater awareness at board level. King III, however, provides no detailed guidance with regard to the practical implementation of these principles and practices. It is worth noting that numerous international guidelines are recommended within King III that can be adopted as frameworks to assist in the effective implementation of IT governance. COBIT 5 provides, as part of its governance process practices, related guidance activities linking it to the seven IT governance principles of King III, thus making it a practical framework for the implementation of King III recommendations. This study sought to establish the extent to which the governance processes, practices and activities of COBIT 5 are mapped to the recommended practices of IT governance as highlighted in King III in order to resolve COBIT 5 as the de facto framework for IT governance in terms of King III. The study found that though King III principles and practices may be interpreted as vague with regard to *how* to implement IT governance principles, COBIT 5 succeeds in bridging the gap between control requirements, technical issues, information systems and business risk, which consequently results in a better facilitation of IT governance. The study also revealed that COBIT 5 contains additional activities to assist the board in more transparent reporting of IT performance and conformance management to stakeholders as well activities which enable the connection of resource management with human resources and financial planning.

**Keywords:** Board, IT Governance, King III, COBIT 5, Governance Activities

## 1. INTRODUCTION

Information technology ("IT") is an integral part of an organisation and is incorporated in all aspects of its business processes. Furthermore, it is increasingly evolving to be crucial in the operation, support, sustainability and expansion of the organisation. This means that the management of this important strategic asset, which creates opportunities and provides a competitive edge, is crucial (Van Grembergen, De Haes & Guldentops 2004:2; IoD, 2009:14; Butler & Butler, 2010:33; Nel, 2011:4; Marnewick & Labuschagne, 2011:661; Ali & Green, 2012:179-180). The use of IT has become so pervasive that it can no longer be viewed as just as an enabler to business: it has transformed into the new role of being a strategic partner to business (Van Grembergen, De Haes & Guldentops, 2004:2; IoD, 2009:14). As strategic partner and business enabler, it is difficult to distinguish IT from the organisational strategic mission, because it serves to increase the company's profits and shareholder value (Lainhart & John, 2000:33; Posthumus & Von Solms, 2005:12; Ragphupathi 2007:95; Kaselowski, Von Solms & Von Solms, 2010:336). This link to strategic mission mandates IT governance as a corporative imperative, meaning the management thereof at board level, which results in more effective oversight and alignment of IT with the overall business strategy of the organisation (Hardy, 2006:55). Boards who undertake such oversight understand their corporate accountability and responsibility, which emanates in proactive leadership (Posthumus & Von Solms, 2005:17). The board, tasked by King III with the responsibility of governing risk, therefore ought to be keenly aware of the potential harms embedded in the organisations' value-creating activities, such as IT, and should be pro-active in showing leadership and strategic control in guiding efforts to meet risk management expectations (IoD, 2009:85; Weitzner & Peridis, 2011:34).

These strategic control measures should consist of the specific leadership, organisational structures and processes that ensure that the organisation's IT sustains and extends its strategy and objectives (De Haes and Van Grembergen, 2008). Owing to the complexity of IT and the general lack of understanding of it, the management of IT is often treated as a separately managed "value providing asset" and rarely receives the necessary attention of the board. This creates what is "a basic

disconnect between boards and the IT" (Ragphupathi, 2007:95). The result of this is that many executives are intimidated by the task of managing technology, because their mind set is that IT requires "special tools, special strategies and a special mind set" (Bensaou & Earl, 1998:120). This mind set is promoted by a general lack of understanding by the board of IT controls, a vacuum of technical insight required to manage IT in comparison to other strategic disciplines and the unavailability of formal guidance which assists the board in effectively executing its responsibilities towards IT (Damianides, 2005:81; Butler & Butler, 2010:34, Marnewick & Labuschagne, 2011:669).

King III includes a chapter providing guidelines to the board in relation to the effective governance of this important strategic activity. This code, however, only provides principles and recommended practices to effective IT governance in order to create a greater awareness of IT governance at board level (IoD, 2009:15); no detailed guidance is provided in terms of implementation. Given this limited guidance provided coupled with an apparent lack of board involvement in IT-related matters, the risk arises that board members may lack the fundamental knowledge needed to ask intelligent questions regarding IT governance, which will result in the delegation of IT governance to the Chief Information Officer (CIO) of the organisation and the governance of IT therefore being managed in an ad hoc manner (Nolan & McFarlan, 2005:1). These actions would circumvent the principle set by King III which necessitates the involvement of the board in making IT-related decisions in order to foster a systematic and repeatable approach to desirable behaviour (Sandiro-Arndt, 2008). The adoption of recognised frameworks of IT governance can assist those charged with governance, such as the board, to attain the advocated goal of effective IT governance. The guidance attained from frameworks ensures that the board, inter alia, is confident of where it is going, understands how to get there, is aware of what to expect along the way and knows when appropriate action needs to be taken (Afzali, Azmayandeh, Nassiri & Shabgahi, 2010:46). The Control Objectives for Information and Related Technology ("COBIT") provides such guidance.

COBIT is widely considered "the de facto standard for IT governance worldwide" (Marnewick & Labuschagne, 2011:668). Now in its fifth edition, it considers itself the framework to be adopted for enterprise-wide governance of IT. COBIT was designed to bridge the gap between technical people and business people by facilitating a common understanding of IT (Kadam, 2012:21). Of particular importance to this study is that COBIT 5 provides, as part of its governance process practices, related guidance activities linking it to the seven IT governance principles of King III.

The study found that COBIT 5's governance process activities mapped almost perfectly to the King III recommended practices and in some instances provided even more value-adding activities than King III.

The remainder of this paper is structure as follows: the next section presents the objectives, scope and limitations underpinning the study; thereafter the theoretical background of this study will be discussed as well as the methodology applied and the empirical findings and deductions. The recommendations drawn from the study and areas identified for future research are presented in the last section.

## 2. OBJECTIVES AND SCOPE

The objective of this paper is twofold: firstly, to provide a brief overview of the emergence of IT governance through King III and the conceptualisation of IT governance with regard to the elements of an effective IT governance platform. Secondly, it aims to provide evidence of COBIT 5's governance process as a framework for effective IT governance in terms of King III. To achieve this objective a literature view was performed to achieve the following: identify the recommendations of King III with regard to effective IT governance; establish the concept "IT governance", the IT governance focus areas and its mechanisms; and endorse the link between IT governance and corporate governance. This review is then supported by empirical evidence obtained from assessing, through comparative analysis, the suitability of the governance process activities of COBIT 5 as IT governance framework for King III.

## 3. THEORETICAL BACKGROUND

### 3.1 The emergence of IT governance through King III

The ease of transacting via the internet, the continued growth of e-commerce and increased online trading ensure that the modern organisation trades more efficiently, instantly. These competitive advantages brought about by the more expansive use of IT inherently increase the risk of IT to the organisation and require it to be controlled and governed at the highest level of management (IoD, 2009:15). Chapter 5 of King III Report and section 5 of the code deal with the governance of IT. King III provides top management with a chapter outlining seven guiding principles behind IT governance, and these are supported by 24 recommended practices. A summary of the principles together with the recommended practices for each principle is provided in Table 1 below. It is worth mentioning that in its introductory chapter to King III, the committee highlighted that "due to the broad and ever evolving nature of the discipline of IT governance, the chapter does not try to be the definitive text on the subject, but rather to create a greater awareness at director level" (IoD, 2009:15). This statement provides credibility to Botha (2014:13), who declares that while the code provides the board with *who* the responsibility of IT governance resides with as well as *what* should be done, the code does not outline *how* this should be done.

**Table 1.** Summary of IT governance principles and recommended practices per King III

| *IT Governance Principle* | *Recommended practice* |
|---|---|
| 5.1. The board should be responsible for IT Governance | 5.1.1. The board should assume responsibility for the governance of IT and place it on the board agenda |
| | 5.1.2. The board should ensure that an IT charter and policies are established and implemented |
| | 5.1.3. The board should ensure the promotion of an ethical culture and awareness of a common IT language |
| | 5.1.4. The board should ensure that an IT internal control framework is adopted and implemented |
| | 5.1.5. The board should receive assurance on the effectiveness of the IT internal controls. |
| 5.2. IT should be aligned with the performance and sustainability objectives of the company | 5.2.1 The board should ensure that the IT strategy is integrated with the company's strategic objectives and business processes. |
| | 5.2.2. The board should ensure that there is a process to identify and exploit opportunities to improve the performance and sustainability of the company through the use of IT. |
| 5.3. The board should delegate to management the responsibility for the implementation of an IT governance framework | 5.3.1. Management should be responsible for the implementation of the structures, processes and mechanisms for the IT governance framework. |
| | 5.3.2. The board may appoint an IT steering committee of similar function to assist with its IT governance |
| | 5.3.3. The CEO should appoint a CIO responsible for the management of IT. |
| | 5.3.4. The CIO should be a suitably qualified and experienced person who should have access to and interact regularly on strategic IT matters with the board and/or appropriate board committee and executive management. |
| 5.4. The board should monitor and evaluate significant IT investments and expenditure | 5.4.1. The board should oversee the value delivery of IT and monitor the return on investment from significant IT projects. |
| | 5.4.2. The board should ensure that intellectual property contained in information systems is protected. |
| | 5.4.3. The board should obtain independent assurance on the IT governance and controls supporting outsourced IT services. |
| 5.5. IT should form an integral part of the company's risk management | 5.5.1 Management should regularly demonstrate to the board that the company has adequate resilience arrangements in place for disaster recovery. |
| | 5.5.2. The board should ensure that the company complies with IT laws and that IT-related rules and codes are considered. |
| 5.6. The board should ensure that information assets are managed effectively | 5.6.1. The board should ensure that there is a system in place for the management of information, including information security, information management and information privacy |
| | 5.6.2. The board should ensure that all personal information is treated by the company as an important business asset and identified. |
| | 5.6.3. The board should ensure that an Information Security Management system is developed and implemented. |
| | 5.6.4. The board should approve the information security strategy and delegate and empower management to implement the strategy. |
| 5.7. A risk committee and audit committee should assist the board in carrying out its IT responsibilities | 5.7.1. The risk committee should ensure that IT risks are adequately addressed. |
| | 5.7.2. The risk committee should obtain appropriate assurance that controls are in place and effective in addressing IT risks. |
| | 5.7.3. The audit committee should consider IT as it relates to financial reporting and the going concern of the company. |
| | 5.7.4. The audit committee should also consider the use of technology to improve audit coverage and efficiency. |

*Source: IoD (2009: 39-41)*

## 3.2. Conceptualising IT Governance

### *3.2.1. Defining IT Governance*

IT governance lacks a shared definition because the term "IT governance" has rapidly advanced and the literature provides many definitions thereof (Lee & Lee, 2009:47, Simonsson & Johnson, 2006, Coertze & Van Solms, 2013:3359). The definition adopted for the purposes of this study is that "IT governance is the clarification of decision-making rights and responsibilities as companies seek to leverage IT assets to business goals. This alignment is designed to allow organisations to achieve their goals through putting in place a systematic series of activities establishing structures and processes" (Lee & Lee, 2009:48).

### *3.2.2. The focus areas of IT Governance*

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

- *Strategic alignment* involving making certain that business and IT plans are linked together; defining, maintaining and validating the IT value proposition; and aligning IT operations with overall business operations.
- *Value delivery* dealing with executing the value proposition throughout the delivery cycle, making certain that IT delivers its promised benefits against strategy, focusing on optimising costs and verifying the inherent value of IT.
- *Risk management* necessitating risk awareness by senior corporate officers, a clear understanding of the organisation's risk appetite, and understanding of compliance requirements, transparency regarding significant organisational risks and embedding of risk management responsibilities in an organisation.
- *Resource management* is concerned with the best possible investment in, and the appropriate management of vital IT resources, which would include applications, information, infrastructure and people. Some important points of concern relate to the optimisation of knowledge and the infrastructure.
- *Performance measurement* tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using tools such as balanced scorecards that transform strategy into action to achieve goals measurable beyond traditional accounting.

### *3.2.3. IT Governance Mechanisms*

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

#### *3.2.3.1. Governance structures (who makes the decisions and who is held accountable)*

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

#### *3.2.3.2. Governance processes (how decisions are made?)*

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

- *IT principles*: Decides on questions such as the role of IT and the basis of the funding of IT projects;
- *IT architecture*: Discusses the way in which the core business processes are implemented in IT;
- *IT infrastructure strategies*: Decides on the set of IT infrastructure services needed to support the company's strategic objectives;
- *Business application needs*: Determines the set of business applications needed to support the company's business objectives;
- *IT investment and prioritisation*: Ensures that the IT investment continues to support the company's changing needs.

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

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

## 3.3. IT Governance and the Board

An effective board understands what its role in the organisation is and ensures that it executes the organisation's strategic objectives. Embracing IT oversight as part of its fiduciary duties is indicative of the board's leadership, accountability and responsibility (Posthumus & Von Solms, 2005:17), because this demonstrates foresight in

understanding the enormous impact IT has on strategic decision-making. "Governing technology investment and risk has become part of a board's fiduciary duty of care whether boards realise it or not" (Valentine, 2014:1). King III places this responsibility on the shoulders of the board.

A clearer understanding of IT strategy improves the organisation's internal control system, resulting in better support for overall corporate governance objectives (Posthumus & Von Solms, 2005:17). The literature supports this, purporting that the control formulation and implementation of IT strategy, which underpins IT governance, is the responsibility of the board of directors and forms part of corporate governance (De Haes & Van Grembergen, 2004; Parent & Reich, 2009:135; Spremic, 2009:910; Saetang & Haider, 2011:79-80). IT governance is not only a function of conventional corporate governance but forms part of the board's broader governance responsibilities, known as enterprise governance (Lainhart, 2000:33; Weill, 2004; Damianides, 2005:81; Chalaris, Lemos & Chalaris, 2005; Raghuphati, 2007:96; ISACA 2012, Valentine, 2014:1).

### *3.3.1. Enterprise governance*

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

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

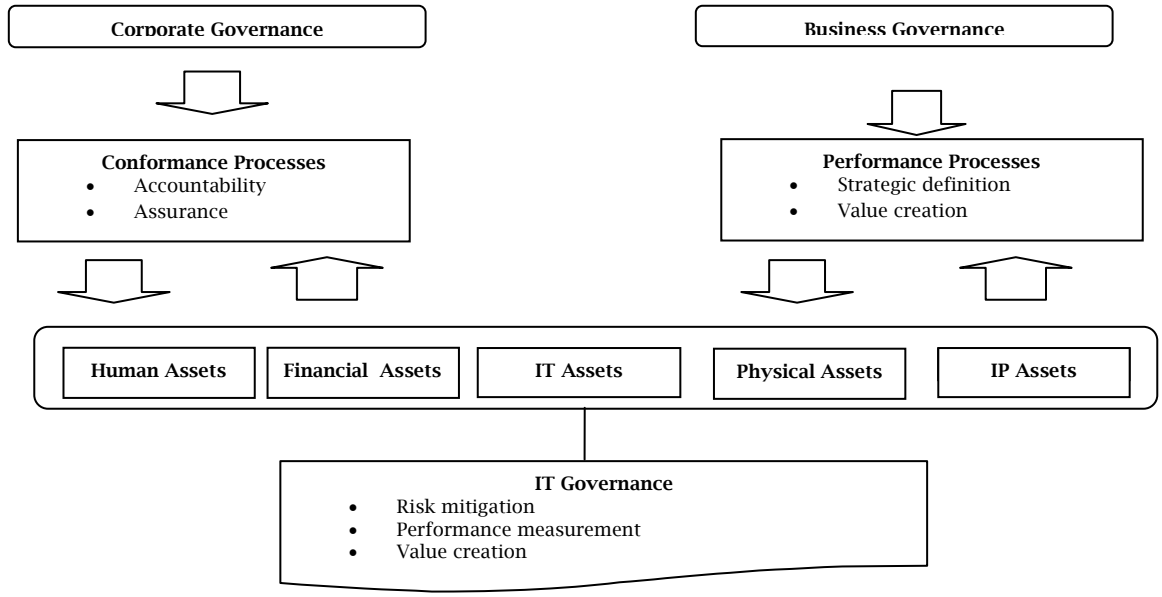
The conformance dimension is concerned with policies, plans and regulation, whereas the performance dimension is concerned with strategy formulation, policy-making and formulating guidelines to direct management decision-making (Elgharbawy & Adbel-Kader, 2013:101). These dimensions should be viewed as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

IT influences the strategic direction envisaged by the board for the organisation, as the organisation requires IT activities to meet its business objectives (Lainhart, 2000:34). An interdependence can therefore be established, resulting in IT governance forming a sub-set of the overall governance responsibilities of the board. This interdependence is illustrated in Figure 1.

### *3.3.2. Effective IT governance is the responsibility of the board*

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

**Figure 1.** Enterprise Governance Framework




*Source: Sandiro-Arndt (2008)*

According to Van Grembergen, De Haes and Guldentops (2004:6), the pertinent questions on IT governance the board must at all times have adequate information on and be able to respond to are:

- How does the board get the CIO and IT organisation to return some business value to organisation at large?

• How does the board make sure that the CIO and IT organisation do not steal the capital supplied or make bad investment decisions therewith?

• How does the board maintain control over CIO and the IT organisation at large?

These questions ensure the establishment of a better control environment over IT, and since corporate governance is the system through which companies are controlled, and control is exercised by senior management within the company aiming to achieve predetermined goals, IT governance is implicitly a dimension of risk management and control, which is once again a responsibility of the board (Aka, 2007:238; Satidularn, Wilkin, Tanner, Linger, 2013:421; Rubino & Vitolla, 2014:320).

### 3.4. COBIT: A Framework for IT Governance

The growth in reliance upon IT has necessitated that the board adopt a more focused approach towards IT governance (IoD, 2009:14-15). To achieve such a focused approach, the board should attain a thorough understanding around the issues and strategic importance of IT in sustaining the operations of the organisation and in so doing ensure that its responsibility toward IT governance yields the required returns in terms of IT alignment and IT-related risks being effectively managed (Hardy, 2006:56).

Whilst being well aware of how essential IT is to their organisation, boards have been slow to embrace their responsibility towards IT governance, and this has placed them at risk of "flying blind" (Valentine, 2014:3) as a result of tending to have little interest in IT coupled with little or no expertise in it (Raghuphati, 2007:95). Further exacerbating the effective implementation of IT governance is that board members are not provided with specific guidance on how to achieve the vaunted goal of effective IT governance (Hardy, 2006:56). The necessary guidance can be provided in the form of a comprehensive framework which will assist in the establishment and assessment of control processes, resulting in better implementation of IT governance (Rezaei, 2013:82). The absence of such a comprehensive and sound IT governance framework compounds the complexities of modern systems, which can then overwhelm the board (Tuttle & Vandervelde, 2007:241).

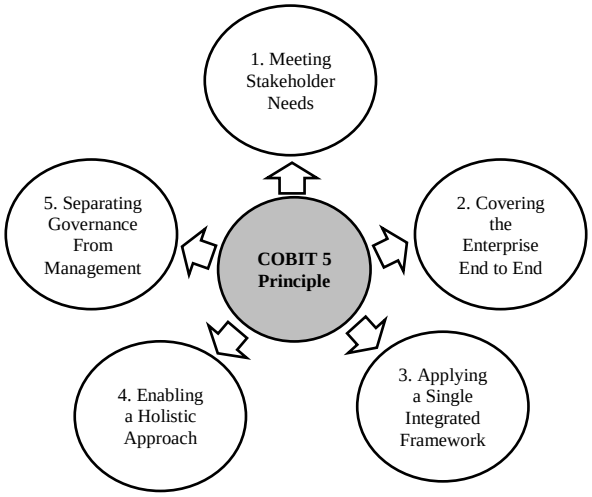
COBIT constitutes such guidance, as it is an IT governance tool that bridges the gap between control requirements, technical issues, information systems and business risk in order to facilitate better governance of IT (Lainhart, 2000:22; Hardy, 2006:59; Rubino & Vitolla, 2014:326).

#### *3.4.1. COBIT 5*

COBIT was developed by the Information Systems Audit and Control Association (ISACA), and the international professional membership association for IT professionals and auditors, through the IT Governance Institute (ITGI), as a set of best practices for information technology management (Sahibudin, Sharifi & Ayat, 2008:749; Rouyet-Ruiz, 2008:41; De Haes & Van Grembergen, 2012). Now in its fifth version, released in April 2012, COBIT conceptualises itself as the enterprise governance of IT. ISACA positions COBIT 5 to be a "comprehensive framework that assists enterprises to achieve their objectives for the governance and management of enterprise IT. COBIT 5 enables IT to be governed and managed in a holistic manner for the whole enterprise, taking in the full end to end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders" (ISACA, 2012).

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

**Figure 2.** COBIT 5 Principles




*Source: ISACA, 2012*

#### *3.4.2. COBIT governance proecess*

COBIT 5 draws on guidance provided in ISO 38500, the ISO standard for the "Corporate Governance of IT", to organise all governance-related processes under one domain (De Haes, Van Grembergen, & Debreceny, 2013:317). These processes require *Evaluate, Direct and Monitor (EDM)* practices, which necessitates the involvement of the board of directors in IT governance (De Haes & Van Grembergen, 2012:100; Oliver & Lainhart, 2012:9). COBIT 5 sets about achieving effective governance by ensuring enterprise objectives such as "evaluating stakeholder needs; setting direction through prioritisation and decision making; and monitoring performance, compliance, and progress against plans" are realised (De Haes, et al., 2013:317). These objectives form part of broader stakeholder objectives, which, according to COBIT 5, should be achieved by way of an effective governance process through which "practices and activities are aimed at evaluating strategic options, providing direction to IT and monitoring the outcome" (ISACA, 2012).

The governance domain of COBIT 5 consists of five governance processes within which EDM practices are suggested. Each governance practice is supported by guidance with regard to how, why and what is to be implemented in order to improve IT performance (ISACA, 2012). COBIT 5 labels the guidance "activities", and provides a set of good practices and standard steps deemed necessary to attain governance. Each of the five governance processes are linked to related guidance areas such as King III to highlight how the principles of King III are being addressed via each process. Botha (2014:4) emphasises that in order for an organisation to implement effective IT governance, an IT governance framework is required that encapsulates structures, processes and mechanism to help the organisation

to meet its overarching objective of creating value for the business. COBIT 5 attempts to be such a framework.

The COBIT 5 processes, together with practices, mapped with King III principles, discussed above, are summarised in Table 2 below. The table details the objective of the each process together with the individual EDM sub-objectives requiring board-level attention:

**Table 2.** COBIT 5 governance processes and activities mapped to King III principles

| | | |
|---|---|---|
| ***EDM01 Ensure Governance Framework Setting and Maintenance*** | | |
| Analysis and articulation of IT governance requirements within the enterprise to ensure IT-related decisions complement the strategies and objectives of the enterprise. It also highlights oversight activities over IT-related processes to ensure that legal, regulatory and board governance requirements are met. | | |
| *EDM01.01 Evaluate the governance system*<br>Establish stakeholder needs, document an understanding of these needs and assess the current and future design of the IT governance within the enterprise. | *EDM01.02 Direct the governance system*<br>Obtain enterprise leaders' buy-in and support and direct governance structures, processes and practices in accordance with agreed-upon decision-making models, design principles and authority levels. | *EDM01.03 Monitor governance system*<br>Monitoring of effectiveness and performance of enterprise IT governance and related mechanisms (structures, processes and principles). |
| *King III related principle(s)*<br>5.1. The board should be responsible for information technology (IT) governance.<br>5.3. The board should delegate to management the responsibility for the implementation of an IT governance framework | | |
| ***EDM02 Ensure benefit delivery*** | | |
| Optimisation of return on investment obtained by the organisation from IT services, IT assets and business processes and cost-efficient delivery of services and solutions. | | |
| *EDM02.01 Evaluate value optimisation*<br>Continual evaluation of IT investments, services and assets in delivering enterprise objectives at a reasonable cost. | *EDM02.02 Direct value optimisation*<br>Channel value management principles and practices towards optimal value creation. | *EDM02.03 Monitor value optimisation*<br>Monitoring of key indicators to determine the extent to which expected value and benefits are derived from IT-related investments and services. |
| *King III related principle(s)*<br>5.2. IT should be aligned with the performance and sustainability objectives of the company<br>5.4. The board should monitor and evaluate significant investments and expenditure. | | |
| ***EDM03 Ensure Risk Optimisation*** | | |
| Ensures that risk appetite of enterprise is not exceeded, IT risk is identified and managed and compliance failures minimised. | | |
| *EDM03.01 Evaluate risk management*<br>Evaluation of risk in terms of the use of IT for the enterprise as well as an assessment of the appropriateness of the risk appetite being adopted. | *EDM03.02 Direct risk management*<br>Direct risk management practices to gain assurance that actual IT risk does not exceed enterprise risk appetite. | *EDM03.03 Monitor risk management*<br>Monitor key goals and metrics of risk management processes and establish how problems will be identified, tracked and reported |
| *King III related principle(s)*<br>5.5. IT should form an integral part of the company's risk management.<br>5.7. A risk committee and audit committee should assist the board in carrying out its IT responsibilities. | | |
| ***EDM04 Evaluate Resource Optimisation*** | | |
| Ensure resource needs (people, processes and technologies) are met in the optimal manner and IT costs are optimised | | |
| *EDM04.01 Evaluate resource management*<br>Continually establish current and future IT resources, options for resourcing and allocation and management principles to meet needs of enterprise. | *EDM04.02 Direct resource management*<br>Ensure the adoption of resource management principles to enable optimal use of IT resources throughout their full economic life cycle. | *EDM04.03 Monitor resources management*<br>Monitor the key goals and metrics of the resource management processes and establish how deviations or problems will be identified, tracked and reported for remediation. |
| *King III related guidance*<br>5.6. The board should ensure that information assets are managed effectively. | | |
| ***EDM05 Ensure Stakeholder Transparency*** | | |
| Ensure that enterprise IT performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and the necessary remedial actions. | | |
| *EDM05.01 Evaluate stakeholder reporting requirements*<br>Continually examine and make judgements on the current and future requirements for stakeholder communication and reporting, including both mandatory reporting requirements (e.g. regulatory) and communication to other stakeholders. Establish the principle for communication. | *EDM05.02 Direct stakeholders communication and reporting*<br>Ensure the establishment of effective stakeholder communication and reporting, including mechanisms for ensuring the quality and completeness of information, oversight of mandatory reporting, and creating a communication strategy for stakeholders. | *EDM05.03 Monitor stakeholder communication*<br>Monitor the effectiveness of stakeholder communication. Assess mechanisms for ensuring accuracy, reliability and effectiveness, and ascertain whether the requirements of different stakeholders are met. |
| *King III related principle(s):*<br>None | | |

*Source: ISACA, 2012*

## 4. METHODOLOGY

The literature review provided the foundation for the aspects tested by means of a comparative analysis whereby the 24 best-practice recommendations as provided by King III are mapped against the 79 governance activities suggested in terms of COBIT 5. This was done to

determine the extent to which the best-practice recommendations of King III are addressed by COBIT 5's governance process. The mapping done distinguishes the role the board needs to fulfil in terms of COBIT 5, viz. evaluate, direct or monitor with regard to each recommended principle of King III.

An assessment was done based on King III-recommended practices not addressed in COBIT 5 to ascertain the completeness of COBIT 5 as an IT governance framework for King III purposes. This exercise was also performed on activities addressed in COBIT 5 for which no recommended practice was suggested by King III to determine whether these activities could possibly strengthen an organisation's governance of IT. Appendix 1 contains a detailed mapping of King III's IT governance principles supported by its recommended practices (i.e. *what* should be done) to COBIT 5's governance process activities, which provides practical implementation guidance (i.e. *how* it should be done).

## 5. RESEARCH FINDINGS AND INTERPRETATIONS

This section presents the findings of the comparative analysis of King III's 24 best-practice recommendations to COBIT 5's governance process activities. The detailed mapping results are contained in Appendix 1.

### 5.1. Governance activities addressed by COBIT 5 but not by King III

#### *5.1.1. EDM05 Ensure Stakeholder Transparency*

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

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

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

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

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

#### *5.1.2. Alignment of resource management with financial and human resources (HR) planning*

COBIT 5 addresses governance activities, highlighting the need for board involvement in terms of connecting resource management with HR and financial planning. The sentiment expressed in COBIT is that in the process of IT resource planning/management, it is of the utmost importance that an organisation takes into account its financial and human capital resources. King III in principle 5.6. addresses the management of information assets but fails to link these important elements of effective resource planning to the related recommended practice.

### 5.2. Recommended practices addressed by King III but not by COBIT 5

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

III as part of principle 5.1 highlights that the organisation "should understand and manage the risk, benefits and constraints of IT" (IoD, 2009:82). Furthermore, the code requires good governance principles of enforcement and monitoring of effective IT governance even where the provision of IT goods and services has been outsourced (IoD, 2009:85). COBIT 5 governance activities do not directly address this recommended practice. It is, however, worth mentioning that though not addressed directly, COBIT does state that the board should "monitor IT sourcing strategies, enterprise architecture strategies, IT resources and capabilities to ensure that current and future needs of the enterprise are met" (ISACA, 2012). However, this activity does not address the element of obtaining assurance regarding outsourced services and consequently fails to address the recommended practice adequately.

### 5.3. Summative findings

The findings of the comparative analysis discussed above in sections 5.1. and 5.2. indicate that COBIT 5 requires the board to ensure that IT performance and conformance management and the reporting thereof are transparent and measurable by stakeholders against set goals and metrics. The recommended practices provided by King III can be vague at times, and hence there is a possibility that this activity is addressed as part of practices 5.1.5, 5.5.2 of King III. A more definitive incorporation of these activities into King III can yield the results of:

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

COBIT 5 also highlights the need for connecting resource management with HR and financial planning. Principle 5.6 does address management of

information assets but fails to link these important elements of effective resource planning to their related recommended practice.

King III, in comparison, requires the board to attain an understanding of the IT risks, benefits and constraints and to effectively manage these. It also requires the existence of good governance principles surrounding the outsourcing of IT goods and services. Though not specifically addressed in the level of detail set out in King III, COBIT 5 makes reference to the monitoring of IT sourcing strategies, resources and enterprise architecture strategies. It must however be noted that the governance domain activities do not make reference to the attainment of independent assurance on the IT governance and controls supporting outsourced IT services.

## 6. RECOMMENDATIONS AND AREAS FOR FUTURE RESEARCH

Based on the results of the study, it is recommended that the boards of South African organisations give careful consideration to adopting COBIT 5 as their framework for IT governance. The recommendation is supporting by the evidence that COBIT 5 is not only aligned to the IT governance principles recommended by King III, but its governance process activities maps near perfectly to the recommended practices of King III.

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

## 7. CONCLUSIONS

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

## REFERENCES


1. Afzali, P., Azmayandeh, E., Nassiri, R., & Shabgahi, G. L. (2010, November). *Effective governance through simultaneous use of COBIT and Val IT. International Conference on Education and Management Technology*: 46-50
2. Aka, PC. (2007). Corporate Governance in South Africa: Analyzing the Dynamics of Corporate Governance Reforms in the "Rainbow Nation". *North Carolina Journal of International Law and Commercial Regulation,* 33: 220 – 292.
3. Ali, S., & Green, P. (2012). Effective information technology (IT) governance mechanisms: An IT outsourcing perspective. *Information Systems Frontiers,*14(2), 179 – 193.
4. Almeida, R., Pereira, R., & da Silva, MM. (2013). IT Governance Mechanisms: A Literature Review. In Exploring Services Science: 186 – 199. Springer Berlin Heidelberg.
5. Bensaou, BM., & Earl, M. (1998). Information Technology in Japan: Are there Lessons for the West?. *In Information Technology and Industrial Competitiveness.* 153 – 174. Springer US.
6. Bhattacharjya, J., & Chang, V. (2009). *Adoption and Implementation of IT Governance: Cases from Australian Higher Education. In Information Technology Governance and Service Management: Frameworks and Adaptations: 82-100.* Edited by A. Cater-Steel. Hershey, PA: Information Science Reference. doi:10.4018/978-1-60566-008-0.ch003
7. Botha, DP. (2014). *Bridging the Information Technology (IT) gap in South Africa through a step by step approach to IT governance.* (Master's dissertation). Stellenbosch: Stellenbosch University. Available from: http://scholar.sun.ac.za/handle/10019.1/86464
8. Butler, R. & Butler, MJ. (2010). Beyond King III: Assigning accountability for IT governance in South African enterprises. *South African Journal of Business,* 41(3): 33 – 45.
9. Chalaris, I., Lemos, PP., & Chalaris, M. (2005). IT Governance: The Safe Way to Effective and Efficient Governance. *E-Journal of Science and Technology,* 1(1), 59 -63.
10. Coertze, J., & von Solms, R. (2013). The Board and IT Governance: A Replicative Study. *African Journal of Business Management,* 7(35): 3358-3373.
11. Damianides, M. 2005. Sarbanes-Oxley and IT governance: New guidelines on IT control and compliance, *Information Systems Management,* 22(1): 77-85.
12. De Haes, S., & Van Grembergen, W. (2004). IT governance and its mechanisms. Available from: http://pdf.aminer.org/000/245/098/introduction_to_the_minitrack_it_governance_and_its_mechanisms.pdf
13. De Haes, S. & Van Grembergen, W. (2008). Practices in IT Governance and Business /IT Alignment. *Information Systems Control Journal,* Volume 2
14. De Haes, S., & Van Grembergen, W. (2012). An Academic Exploration into the Core Principles and Building Blocks of COBIT 5. *International Journal of IT/Business Alignment and Governance,* 3(2): 51-63.
15. De Haes, S., Van Grembergen, W., & Debreceny, RS. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems,* 27(1):307 – 324.
16. Elgharbawy, A., & Abdel-Kader, M. (2013). Enterprise governance and value-based management: a theoretical contingency framework. *Journal of Management & Governance,* 17(1): 99 – 129.
17. Hardy, G. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security technical report,* 11(1): 55 – 61.
18. Institute of Directors. (IoD). (2009). *King III Report on Corporate Governance*, Institute of Directors in Southern Africa. Johannesburg
19. ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.* Rolling Meadows, IL: ISACA
20. Johnston, AC., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM,* 52(1): 126 – 129.
21. Kadam, AW. (2012, September). The Evaluation of COBIT. *CSI Communications:* 21 – 22.
22. Kaselowski, E., Von Solms, B., & Von Solms, R. (2010). Municipalities and information technology

governance-towards a strategic planning framework. *Journal of Public Administration,* 45(2): 334 – 342.
23. Kordel, L. (2002). IT Governance Hands-on: Using Cobit to Implement IT Governance. *Information Systems Control Journal,* Vol 2.
24. Kurti, I., Barrolli, E., & Sevrani, K. (2014). Effective IT Governance in the Albanian Public Sector – A Critical Success Factors Approach. *The Electronic Journal of Information Systems in Developing Countries,* 63(6): 1-22.
25. Lainhart, IV. (2000). COBIT™: A methodology for managing and controlling information and information technology risks and vulnerabilities. *Journal of Information Systems,* 14(1): 21-25.
26. Lainhart, IV., & John, W. (2000). Why IT governance is a top management issue. *Journal of Corporate Accounting & Finance,* 11(5): 33-40.
27. Lee, J., & Lee, C. (2009). *IT Governance-Based IT Strategy and Management: Literature Review and Future Research Directions. In Information Technology Governance and Service Management: Frameworks and Adaptations*: 44-62. Edited by A. Cater-Steel. Hershey, PA: Information Science Reference. doi:10.4018/978-1-60566-008-0.ch002
28. Marnewick, C., & Labuschagne, L. (2011). An investigation into the governance of information technology projects in South Africa. *International Journal of Project Management,* 29(6):661-670.
29. Musson, D. (2009). IT Governance: A Critical Review of the Literature. In Information Technology Governance and Service Management: Frameworks and Adaptations: 63-81. Edited by Cater-Steel (Ed.). Hershey, PA: Information Science Reference. doi:10.4018/978-1-60566-008-0.ch003
30. Nel, I. (2011). *An investigation into the business continuity risks and related business continuity plan* (Masters Dissertation). Auckland Park, Johannesburg: University of Johannesburg. Available from: http://hdl.handle.net/10210/5067
31. Nolan, F. & McFarlan, FW. (2005). Information Technology and the Board of Directors. *Harvard Business Review.* Available from: http://www3.fsa.br/LocalUser/gestaoti/Ativ03%20NOLAN%202005%20%20Information%20Technology%20and%20the%20Board%20of%20Directors..pdf
32. Parent, M., & Reich, B. H. (2009). Governing Information Technology Risk. *California Management Review,* 51(3):134-152.
33. Posthumus, S. & Von Solms, R. (2005). IT oversight: an important function of corporate governance. *Computer Fraud & Security,* 2005(6): 11-17.
34. Posthumus, S., von Solms, R. & King, M. (2010). The board and IT governance: The what, who and how. *South African Journal of Management,* 41(3):23-32.
35. Raghupathi, W. (2007). Corporate Governance of IT: A Framework for Development. *Communications of the ACM,* 50(8):94 – 99.
36. Rezaei, N. (2013). The Evaluation of Implementing IT Governance Controls. *Journal of Applied Business and Finance Researches*, *2*(3): 82-89.
37. Rouyet-Ruiz, J. (2008). COBIT as a Tool for IT Governance: between Auditing and IT Governance. *The European Journal for the Informatics Professional,* 9(1): 40-43.
38. Rubino, M., & Vitolla, F. (2014). Corporate governance and the information system. How a framework for IT governance supports ERM. *Corporate Governance,* 14(3): 320-338.
39. Saetang, S., & Haider, A. (2011). *Conceptual aspects of IT governance in enterprise environment. Proceedings of the 49th SIGMIS annual conference on Computer personnel research*: 79-82.
40. Sahibudin, S., Sharifi, M., & Ayat, M. (2008). *Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. Second Asia International Conference on Modelling and Simulation:* 749-753.
41. Sandiro-Arndt, B. (2008). People, Portfolios and Processes: The 3P Model of IT Governance. *Information Systems Control Journal,* 2:36-39.
42. Satidularn, C., Wilkin, C., Tanner, K., & Linger, H. (2013). Investigation of the Relationship between IT Governance and Corporate Governance. *Management, Leadership and Governance,* 420–423.
43. Simonsson, M., & Johnson, P. (2006, June). *Defining IT governance-a consolidation of literature. In the 18th Conference on Advanced Information Systems Engineering.* Available from: http://www.ics.kth.se/Publikationer/Working%20Papers/EARP-WP-2005-MS-04.pdf
44. Simonsson, M. & Ekstedt, M. (2006). *Getting the Priorities Right: Literature vs Practice on IT Governance. Proceedings of the Technology Management for the Global Future (PICMET),* Portland, USA.
45. Spremic, M. (2009). IT Governance Mechanisms in Managing IT Business Value. *Information Science and Applications,* 6(6):906-915.
46. Tuttle, B., & Vandervelde, SD. (2007). An empirical examination of CobiT as an internal control framework for information technology. *International Journal of Accounting Information Systems,* 8(4): 240-263.
47. Valentine, E. (2014). Are Boards Flying Blind When it Comes to Enterprise Technology Governance? *EDPACS,* 49(2):1-5.
48. Van Grembergen W, De Haes S, Guldentops E. (2004). Structures, processes and relational mechanisms for IT governance. *Strategies for Information Technology Governance.* Hershey, PA: Idea Group Publishing: 1-36.
49. Webb, P., Pollard, C. & Ridley, G. (2006). Attempting to Define IT Governance: Wisdom or Folly?. Available from: http://18.7.29.232/bitstream/handle/1721.1/1846/4237-02.pdf?sequence=2
50. Weitzner, D. & Peridis, T. (2011). Corporate Governance as Part of the Strategic Process: Rethinking the Role of the Board. *Journal of Business Ethics,* 102:33-42.
51. Weill, P., & Woodham, R. (2003). Don't just lead, govern: Implementing effective IT governance. Available from: http://18.7.29.232/bitstream/handle/1721.1/1846/4237-02.pdf?sequence=2
52. Weill, P. (2004). Don't just lead, govern: How top-performing firms govern IT. *MIS Quarterly Executive,* 3(1): 1-17.

## Appendix 1

**Table A.1.** Mapping of King III recommended practices to COBIT 5 governance activities

| *IT Governance Principle per King III* | *Recommended Practice as per King III (What should be done)* | *COBIT 5 Practice* | *COBIT 5 Governance Activity Evaluate* | *COBIT 5 Governance Activity Direct* | *COBIT 5 Governance Activity Monitor* |
|---|---|---|---|---|---|
| ***What should be done?*** | | ***How it should be done*** | | | |
| 5.1. The board should be responsible for IT governance. | 5.1.1. The board should assume responsibility for the governance of IT and place it on the board agenda. | EDM01.01<br>EDM01.02<br>EDM01.03 | Analyse and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence governance design.<br>Determine the significance of IT and its role with respect to the business.<br>Consider external regulations, laws and contractual obligations and determine how they should be applied within the governance of enterprise IT.<br>Articulate principles that will guide the design of governance and decision making. | Communicate governance of IT principles and agree with executive management on the way to establish informed and committed leadership. | Assess the effectiveness of the governance design and identify actions to rectify deviations. |
| | 5.1.2. The board should ensure that an IT charter and policies are established and implemented. | EDM01.01<br>EDM01.02<br>EDM01.03 | Understand the enterprise's decision-making culture and determine the optimal decision-making model for IT. | Direct that staff follow relevant guidelines for ethical and professional behaviour and ensure that the consequences of non-compliance are known and enforced. | Maintain oversight of the extent to which IT satisfies obligations (regulatory, legislation, common law, contractual), internal policies, standards and professional guidelines.<br>Monitor regular and routine mechanisms for ensuring that the use of IT complies with relevant obligations (regulatory, legislation, common law, contractual), standards and guidelines. |
| | 5.1.3. The board should ensure the promotion of an ethical culture and awareness of a common IT language. | EDM01.01<br>EDM01.02<br>EDM01.03 | Align the ethical use and processing of information and its impact on society, natural environment, internal and external stakeholder interest with the enterprise's direction, goals and objectives. | Direct the establishment of a reward to promote desirable cultural change. | Maintain oversight of the extent to which IT satisfies obligations (regulatory, legislation, common law, contractual), internal policies, standards and professional guidelines. |
| | 5.1.4. The board should ensure than an IT internal control framework is adopted and implemented. | EDM01.01<br>EDM01.02<br>EDM01.03 | Determine the implications of the overall enterprise control with regard to IT. | Establish or delegate the establishment of governance structures, processes in line with agreed upon design principles. | Periodically assess whether agreed-on governance of IT mechanisms (structures, principles, processes, etc) are established and operating effectively. |
| | 5.1.5. The board should receive assurance on the effectiveness of the IT internal controls. | EDM01.03 | | | Provide oversight of the effectiveness of, and compliance with, the enterprise's system of control.<br>Assess the effectiveness and performance of those stakeholders given delegated responsibility and authority for governance of enterprise IT. |

**Table A.1.** Mapping of King III recommended practices to COBIT 5 governance activities (continued)

| *IT Governance Principle per King III* | *Recommended Practice as per King III (What should be done)* | *COBIT 5 Practice* | *COBIT 5 Governance Activity Evaluate* | *COBIT 5 Governance Activity Direct* | *COBIT 5 Governance Activity Monitor* |
|---|---|---|---|---|---|
| ***What should be done?*** | | ***How it should be done*** | | | |
| 5.2. IT should be aligned with the performance and sustainability objectives of the company. | 5.2.1 The board should ensure that the IT strategy is integrated with the company's strategic objectives and business processes. | EDM02.01<br>EDM02.03 | Evaluate how effectively the enterprise and IT strategies have been integrated and aligned with enterprise goals for delivering value.<br>Consider how well the management of IT-enabled investments, services and assets aligns with the enterprise value management and financial management practices. | | Obtain regular and relevant portfolio, programme and IT (technological and functional) performance reports. Review the enterprise's progress towards identified goals and the extent to which planned objectives have been achieved, deliverables obtained, performance targets met and risk mitigated. |
| | 5.2.2. The board should ensure that there is a process to identify and exploit opportunities to improve the performance and sustainability of the company through the use of IT. | EDM02.01<br>EDM02.02 | Understand and regularly discuss the opportunities that could arise from enterprise change enabled by current, new or emerging technologies, and optimise the value created from those opportunities. | Direct management to consider potential innovative uses of IT that enable the enterprise to respond to new opportunities or challenges, undertake new business, increase competitiveness or improve processes.<br>Recommend consideration of potential innovations, organisational changes or operational improvements that could drive value for the enterprise from IT-enabled initiatives. | |
| 5.3. The board should delegate to management the responsibility for the implementation of an IT governance framework. | 5.3.1. Management should be responsible for the implementation of the structures, processes and mechanisms for the IT governance framework. | EDM01.02<br>EDM01.03 | | Establish or delegate the establishment of governance structures, processes in line with agreed upon design principles. | Periodically assess whether agreed-on governance of IT mechanisms (structures, principles. processes, etc.) is established and operating effectively. |
| | 5.3.2. The board may appoint an IT steering committee of similar function to assist with its IT governance. | EDM01.01<br>EDM01.02<br>EDM01.03 | Determine the appropriate levels of authority delegation, including threshold rules, for IT decisions. | Communicate governance of IT principles and agree with executive management on the way to establish informed and committed leadership. | Assess the effectiveness of the governance design and identify actions to rectify deviations. |
| | 5.3.3. The CEO should appoint a CIO responsible for the management of IT. | | | | |
| | 5.3.4. The CIO should be suitably qualified and experienced person who should have access and interact regularly on strategic IT matters with the board and/or appropriate board committee and executive management. | EDM01.02 | | Ensure that communication and reporting mechanisms provide those responsible for oversight and decision-making with appropriate information. | |

**Table A.1.** Mapping of King III recommended practices to COBIT 5 governance activities (continued)

| *IT Governance Principle per King III* | *Recommended Practice as per King III (What should be done)* | *COBIT 5 Practice* | *COBIT 5 Governance Activity Evaluate* | *COBIT 5 Governance Activity Direct* | *COBIT 5 Governance Activity Monitor* |
|---|---|---|---|---|---|
| ***What should be done?*** | | ***How it should be done*** | | | |
| 5.4. The board should monitor and evaluate significant IT investments and expenditure. | 5.4.1. The board should oversee the value delivery of IT and monitor the return on investment from significant IT projects. | EDM02.01<br>EDM02.02<br>EDM02.03 | Understand what constitutes value for the enterprise, and consider how well it is communicated, understood and applied throughout the enterprise's processes.<br>Evaluate the portfolio of investments, services and assets for alignment with the enterprise's objectives; enterprise worth, both financial and non-financial; risk, both delivery and benefits risks; business process alignment; effectiveness in terms of usability, availability and responsiveness; and efficiency in terms of cost, redundancy and technical health. | Define and communicate portfolio and investment types, categories, criteria and relative weightings to the criteria to allow for overall relative value scores.<br>Define requirements for stage-gates and other reviews for significance of the investment to the enterprise and associated risk, programme schedules, funding plans and the delivery of key capabilities and benefits and ongoing contribution to value.<br>Define and communicate enterprise-level value delivery goals and outcome measures to enable effective monitoring.<br>Direct any required changes to the portfolio of investments and services to realign with current and expected enterprise objectives and/or constraints. | ALL EDM 02.03 activities |
| | 5.4.2. The board should ensure that intellectual property contained in information systems is protected. | EDM02.01<br>EDM04.02 | Understand the key elements of governance required for the reliable, secure and cost-effective delivery of optimal value from the use of existing and new IT services, assets and resources. | Establish principles related to safeguarding resources. | |
| | 5.4.3. The board should obtain independent assurance on the IT governance and controls supporting outsourced IT services. | | | | |

**Table A.1.** Mapping of King III recommended practices to COBIT 5 governance activities (continued)

| *IT Governance Principle per King III* | *Recommended Practice as per King III (What should be done)* | *COBIT 5 Practice* | *COBIT 5 Governance Activity Evaluate* | *COBIT 5 Governance Activity Direct* | *COBIT 5 Governance Activity Monitor* |
|---|---|---|---|---|---|
| *What should be done?* | | *How it should be done* | | | |
| 5.5. IT should form an integral part of the company's risk management. | 5.5.1 Management should regularly demonstrate to the board that the company has adequate resilience arrangements in place for disaster recovery. | EDM03.01<br>EDM03.02<br>EDM03.03 | Determine the level of IT-related risk that the enterprise is willing to take to meet its objectives (risk appetite).<br>Evaluate and approve proposed IT risk tolerance thresholds against the enterprise's acceptable risk and opportunity levels.<br>Determine the extent of alignment of the IT risk strategy to enterprise risk strategy. | Promote an IT risk-aware culture and empower the enterprise to proactively identify IT risk, opportunity and potential business impact.s<br>Direct the integration of IT risk strategy and operations with the enterprise strategic risk decisions and operations. | Monitor the extent to which the risk profile is managed within the risk appetite thresholds. |
| | 5.5.2. The board should ensure that the company complies with IT laws and that IT-related rules, codes are considered. | EDM03.01<br>EDM03.02<br>EDM01.03 | Determine that IT use is subject to appropriate risk assessment and evaluation, as described in relevant international and national standards. | Direct that risk, opportunities, issues and concerns may be identified and reported by anyone at any time. Risk should be managed in accordance with published policies and escalated to the relevant decision-makers. | Monitor regular and routine mechanisms for ensuring that the use of IT complies with relevant obligations (regulatory, legislation, common law, contractual), standards and guidelines. |
| 5.6. The board should ensure information assets are managed effectively | 5.6.1. The board should ensure that there is a system in place for management of information which should include information security, information management and information privacy. | EDM04.01<br>EDM04.02<br>EDM04.03 | Examine and make judgement on the current and future strategy, options for providing IT resources, and developing capabilities to meet current and future needs (including outsourcing).<br>Define the principles for guiding the allocation and management of resources and capabilities so that IT can meet the needs of the enterprise, with the required capability according to the agreed-on priorities and budgetary constraints. | Communicate and drive the adoption of resource management strategies, principles, and agreed-on resources plan and enterprise architecture strategies. | Monitor the allocation and optimisation of resources in accordance with enterprise objectives and priorities using agreed-on goals and metrics.<br>Monitor IT sourcing strategies, enterprise architecture strategies, IT resources and capabilities to ensure that current and future needs of the enterprise can be met. |
| | 5.6.2. The board should ensure that all personal information is treated by the company as an important business asset and identified. | EDM04.01<br>EDM04.02 | Understand the key elements of governance required for the reliable, secure and cost-effective delivery of optimal value from the use of existing and new IT services, assets and resources. | Establish principles related to safeguarding resources | |
| | 5.6.3. The board should ensure that an Information Security Management system is developed and implemented. | EDM04.01<br>EDM04.02 | Define principles for the management and control of the enterprise architecture. | Communicate and drive the adoption of the resource management strategies, principles, agreed-on resource plan. | |
| | 5.6.4. The board should approve the information security strategy and empower management to implement the strategy. | EDM04.02 | | Assign responsibilities for executing resource management. | |

**Table A.1.** Mapping of King III recommended practices to COBIT 5 governance activities (continued)

| *IT Governance Principle per King III* | *Recommended Practice as per King III (What should be done)* | *COBIT 5 Practice* | *COBIT 5 Governance Activity Evaluate* | *COBIT 5 Governance Activity Direct* | *COBIT 5 Governance Activity Monitor* |
|---|---|---|---|---|---|
| ***What should be done?*** | | ***How it should be done*** | | | |
| 5.7. A risk committee and audit committee should assist the board in carrying out its IT responsibilities. | 5.7.1. The risk committee should ensure that IT risks are adequately addressed. | EDM03.01<br>EDM03.02<br>EDM03.03 | Proactively evaluate IT risk factors in advance of pending strategic decisions and ensure that risk-aware enterprise decisions are made. | Direct the development of risk communication plans (covering all levels of the enterprise) as well as risk action plans. | Report any risk management issues to the board or executive committee. |
| | 5.7.2. The risk committee should obtain appropriate assurance that controls are in place and effective in addressing IT risks. | EDM03.01<br>EDM03.02<br>EDM03.03 | Evaluate risk management activities to ensure alignment with the enterprise's capacity for IT-related loss and leadership tolerance of it. | Direct implementation of appropriate mechanisms to respond quickly to changing risk and report immediately to appropriate levels of management, supported by agreed-on principles of escalation (what to report, when, where and how)<br>Identify key goals and metrics of risk governance and management processes to be monitored, and approve the approaches, methods, techniques and processes for capturing and reporting the measurement of information. | Monitor the extent to which the risk profile is managed within the risk appetite thresholds.<br>Monitor the key goals and metrics of risk governance and management processes against targets, analyse the cause of the deviation, and initiate remedial action to address the underlying causes. |
| | 5.7.3. The audit committee should consider IT as it relates to financial reporting and the going concern of the company. | EDM02.01<br>EDM05.03 | Understand and consider how effective current roles, responsibilities, accountabilities and decision-making bodies are in ensuring value creation from IT-enabled investments, services and assets. | | Determine whether the requirements of different stakeholders are met. |
| | 5.7.4. The audit committee should also consider the use of technology to improve audit coverage and efficiency. | EDM02.01<br>EDM05.03 | | | |