The development of an integrated framework in order to address King III's IT governance principles at a strategic level

R. Goosen*
Management Accounting and Auditing, Stellenbosch University,
Private Bag X1, Stellenbosch 7600, Republic of South Africa
Goosen@sun.ac.za

R. Rudman
Auditing and Information Systems, Stellenbosch University,
Private Bag X1, Stellenbosch 7600, Republic of South Africa
RJRudman@sun.ac.za

In today's technologically advanced business environments, Information Technology (IT) has become the center of most businesses' strategic activities. It is for this reason that the King III report has dedicated a chapter to addressing IT governance principles, holding the board of directors (senior management) responsible for addressing such principles. The King III report does provide broad level guidance, however lack sufficient detail on its interpretation. Although various guidelines in the form of IT control frameworks -models and -standards exist, it remains theoretical in nature and companies tend to implement these guidelines in an ad hoc manner. This ad hoc implementation of controls leads to unnecessary controls being implemented, resulting in an ineffective IT governance system that does not address each key strategic risk area.

The objective of this research is to develop an integrated best practices framework, which will provide guidance to senior management in how to effectively and efficiently address King III's IT governance principles by taking a business' unique strategic objectives into account.

A detailed literature review was performed of different control frameworks,-models and standards. These were analysed to identify a list of similar and overlapping control areas. These control areas were thereafter mapped to a list of strategic objectives applicable to most businesses. In doing so, effective and efficient IT governance principles which are understood by senior management, are able to be implemented.

*To whom all correspondence should be addressed.

Introduction

Effective corporate governance principles form the foundation of any successfully managed company. For the past two decades, the King reports have formed the basis for the implementation of good corporate governance practices in South African companies. For the first time the King III report, specifically highlights the importance of addressing strong IT governance principles. The rationale for including IT governance in the King report is emphasised by the changing nature of the IT environments of today's business world, which include extended enterprises, cloud computing, collaboration and big data elements. IT has become an integral part of the day-to-day operations of any business (Institute of Directors Southern Africa (IODSA), 2009), as well as being part of the strategic planning process. Kordel (2004) showed that the extent to which IT supports business decisions and how involved senior management (defined as being part of a management team at the highest level of an organisation holding specific executive powers and higher levels of strategic responsibility than simply, day-to-day activities of the business), is in making important IT decisions will determine how successful a business will be. However, directors appeared to lack the necessary understanding and expertise in dealing with IT control matters (Trites, 2004), choosing to focus mainly on business strategies and risk management procedures (Damianides, 2005). IT matters are often regarded as the IT department's responsibility (Raghupathi, 2007) and seen as a separate functional area, not being managed as an integral part of all business areas (Kordel, 2004). A recent significant development occurred when then King III report stated that directors and senior management should be held overall responsible for the implementation of good IT governance principles. Although the King III report further suggest that these principles are to be delegated to management who are to be responsible for the (operational) implementation of the IT governance framework, the overall understanding and direction with regards to IT governance matters still remain first and foremost management's responsibility at a strategic level (defined as developing strategic objectives which will set the company apart from its competitors and give it its competitive advantage). This however poses a challenge to directors and senior management since King III's guidance on how to practically address IT governance, appear vague and unclear (Muller, 2009) and are only addressed at a high-level.

The problem described above was confirmed by Voogt (2010), who conducted research on how the Chief Financial Officers (CFOs) of the Johannesburg Stock Exchange's (JSE) top 40 companies view their roles and responsibilities with regards to IT matters. The results showed that 52% of these CFOs did not think they were responsible for IT and IT governance matters, whilst 76% did not think it was the CFO's responsibility to manage IT systems and controls. However, the research also showed that these CFOs anticipated that a significantly greater portion of their time would be spent on IT-related matters in future, increasing from a moderate 58% currently, to an anticipated 69%. These statistics emphasise the ever increasing importance of addressing IT governance matters.

A number of best practice IT control frameworks, -models and -standards are available which can be used to develop and implement an effective IT governance system, through which business- and IT-management are required to work together on its implementation. However, a disparity (known as the 'IT gap') has been created arising from the two parties' different understanding and implementation of the control frameworks, -models and –standards, resulting in a misalignment between IT principles to a company's business objectives (Rudman, 2011) and an inefficient IT governance system (Rudman, 2010). In order to overcome this 'IT gap' and the ad hoc implementation of controls, an integrated framework is required to ensure that the practical and effective implementation of IT governance principles in a company is possible. Two matters arise from this: How to effectively address IT governance principles and how to ensure the effective alignment of business objectives with IT governance principles.

Research on establishing an effective IT governance as well as business-IT alignment has been documented by various researchers, but have been addressed separately. In 2006, the Information Technology Governance Institute (ITGI) performed a high level mapping between The Control Objectives for Information and related technology (COBIT) framework's control objectives and *inter alia* the following control guidelines, -frameworks, -models and standards:

- The Committee of Sponsoring Organisations of the Treadway Commission's (COSO) framework,
- The Projects in Controlled Environments (PRINCE II) project management methodology,
- The Code of Practice for Information Security Management (ISO 27002) standard,
- A guide to Project Management Body of Knowledge (PMBOK),
- The TickIT and TOGAF 8.1 methodologies, and
- The Capability Maturity Model Integration (CMMI) model (ITGI, 2006).

In 2008, the ITGI performed a further mapping between the control objectives of the IT best practice control framework COBIT, the control model Information Technology Infrastructure Library (ITIL) and the ISO 27002 standard amongst others (ITGI, 2008a). The ITGI also produced a document discussing the link between IT goals and business goals (ITGI, 2008c).

Smit (2009) attempted to define the mismatch, which exists in this business-IT alignment process. Generic strategic business objectives were identified and these business objectives were aligned to the COBIT's control framework processes. Steenkamp (2011) and Hardy (2006b) showed that, by implementing COBIT's control objectives, a company will, in fact, comply with King III's IT governance requirements, whilst Liell-Cock, Graham and Hill (2009) discussed the alignment between IT governance and the King III report.

The above-mentioned research focuses on how to address IT governance principles and the alignment of business and IT objectives at a strategic level. However, whilst valuable research has been performed in these areas, their effective and practical application has been limited due to the fact that the discussions are mainly theoretical based and only deal with selected aspects of the IT governance alignment process in isolation and do not address these aspects in a combined and integrated manner.

Research objective and motivation

Advice and guidelines on structural, composition, financial and independence matters are readily available to board members and senior management. However, guidance on IT governance matters and IT risk management is not readily available (Hardy, 2006b). This article proposes to address the lack of guidance available to senior management relating to the implementation of IT governance principles provided by the King III report by developing an integrated framework which can be used to practically implement such principles at a strategic level, aligning the control objectives of various IT control frameworks, -models and standards, and in the process achieve alignment with the IT governance principles. This framework can be tailored to a company's unique strategic business objectives. Risk areas can be addressed by implementing the relevant control objectives of a best practice framework at the strategic level, tailored to a company's unique strategic business objectives.

A practical integrated framework would allow senior management to focus on and address the key IT risks as well as strategic areas at the same time. It is the purpose of this research to develop a framework which can be used to link the key control objectives (known as control areas) to strategic business objectives, and in doing so address IT governance principles.

Since every company's strategic business objectives are unique, it is not the purpose of this research to develop a framework which is industry specific, but rather to develop a broad-based framework, which could be adapted to most industries and companies. The research is also limited to IT-related matters, and is thereafter relevant to the IT governance principles.

The findings are most applicable to medium and large sized companies who need to comply with regulatory requirements and have various operational environments which need to be integrated and controlled effectively.

Organisational structure

This research consists of the following sections. Section 2 outlines the research approach followed. A literature review, in section 3, was conducted on the factors that would affect the implementation of a good IT governance system as well as the elements affecting the development of an integrated framework. Section 4 presents the best practice integrated framework that was developed to address IT governance principles at a strategic level. An overview of the research, highlighting the outcomes of the research findings and discussing the implementation of the integrated framework in order to address IT governance requirements at a strategic level is contained in section 5.

Research methodology

IT governance principles are addressed by identifying a company's strategic business objectives (hereafter referred to as a company's 'business imperatives') and implementing of the relevant control objectives which can be tailored to any business, using either an IT control framework, -model and standard or a combination thereof. In order to develop this integrated framework, the following process was followed.

1. A literature review was performed in order to obtain an understanding of the concept of business imperatives as well as various control frameworks, -models and standards. Based on the literature review, the COBIT control framework, the ITIL control model and ISO 27002 (supported by ISO 27001) standards was selected. These were selected since they are internationally recognised and adaptable to most industries and cover the three main areas of control. The COBIT control framework provides guidance for the implementation of IT governance related control objectives and perform a high level risk assessment on the general control environment. The ITIL control model identifies operational risks and provides guidance on how to effectively implement service management principles, whilst the ISO 27001 and ISO 27002 standards address the information security risk matters (Sahibudin, Sharifi & Masarat, 2008). Given the level of detail of these control framework, -model and – standard, this study was limited to identifying internal controls as defined by COSO's definition of an internal control.
2. These three control frameworks, -models and standards were analysed and the control objectives underlying each was combined to identify common control areas (defined as a similar group of controls, which are directed in achieving the same high level control objective of a business).
3. The relevant strategic business imperatives relevant to most businesses were identified from literature.
4. These imperatives were hereafter mapped to each control area to form the basis of the implementable integrated framework in the form of a matrix.

Literature review

In order to perform the mapping between the three selected control frameworks, -models and standards and the strategic business imperatives, an understanding of IT governance and its application had to be obtained.

IT governance

IT governance principles are seen as an integral part of the overall corporate governance structure. According to the King III report, directors should be responsible to take prudent and reasonable steps in order to implement an IT governance framework that supports the effective and efficient management of IT resources, including the implementation of a sound risk management system and internal controls, based on the company's specific requirements, so as to ensure that a company achieves its strategic objectives (IODSA, 2009).

The King III report (IODSA, 2009) highlights seven key IT governance principles that must be implemented in terms of Section 5 of the code.

1 The board should be responsible for information technology governance.
2 IT should be aligned with the performance and sustainability objectives of the entity.
3 The board should delegate to management the responsibility for the implementation of an IT governance framework.
4 The board should monitor and evaluate significant IT investments and expenditure.
5 IT should form an integral part of the entity's risk management process.
6 The board should ensure that information assets are managed effectively.
7 A risk committee and audit committee should assist the board in carrying out its IT duties.

The IT governance framework also includes the human, financial, physical and informational aspects of IT (Doughty & Grieco, 2005).

The following advantages can be expected when strong IT governance practices are implemented:

- A company's reputation is improved, and trust is enhanced with internal parties, such as employees, and external parties, such as customers, suppliers and investors.
- Strong IT governance practices create a competitive advantage aligning IT and business goals and processes, making business operations more efficient and effective.
- Non-IT executives gain a better understanding of IT and improved decision making processes are possible due to relevant and reliable information being available.
- A greater level of compliance with laws and regulations is possible and risk management procedures are maximised (Bowen, Cheung & Rohde, 2007; Hardy, 2006b).

However the risk arises that if these IT governance principles are not implemented, a company is exposed to operational risk as well as a loss in the confidence, integrity, reliability and authenticity in information systems *inter alia*. Gaining unauthorised access, use and changes to the IT systems also becomes a greater risk to a company.

In order to address the IT governance principles and to mitigate these risks, senior management need to take responsibility and certain problem areas need to be addressed such as the 'IT gap' and business-IT alignment.

'IT gap' and business IT alignment

During the implementation of IT governance principles, miscommunication between the senior management (responsible for providing sufficient and effective internal control systems) and IT specialists (responsible for implementing such controls) occurs. This creates a problem, as senior management does not understand the IT *control techniques* (the actual controls implemented to address the identified risks) and technology, whereas IT specialists understand neither the *control frameworks (*a system that covers all fundamental internal controls expected to mitigate the risks), nor the *control models (*providing guidance on the design, implementation and maintenance of such risk controls) that need to be implemented (Rudman, 2008b). This is referred to as the 'IT gap' problem.

In order for a company to successfully overcome this IT gap, a process should be implemented which aligns business goals with IT goals through which a company's strategic business objectives are translated into objectives for the IT department which, in turn will form the basis of the IT strategy (ITGI, 2008b). When these IT objectives are in line with, and support, the business' strategic objectives, the business-IT alignment is achieved (Bleinstein, Cox, Verner & Phalp, 2005), which has the advantages that:

- IT strategies become aligned with and supportive of the strategic business objectives, which reduces the business and IT related risks.
- Reliable real-time data improves decision-making, which leads to better access to new market segments, satisfying new and existing customers' needs and maximising capital investment possibilities (IBM, 2006; Innotas, 2010).

However some businesses still do not comprehend the value and importance of the alignment process (Smit, 2009) and where no alignment or misalignment occurs, it could result in:

- An enterprise fails to meet its business goals, including suffering financial losses, business interruptions, customer dissatisfaction and distrust due to ineffective services and support rendered by the IT function (Bakari, Tarimo, Yngström, Magnusson & Kowalski, 2007).
- Incomplete and inadequate processing and reporting of information due to ineffective and incomplete IT controls (Smit, 2009).
- Excessively high IT costs and overheads occur due to the ineffective use of IT resources (IBM, 2006).

In order to achieve business-IT alignment and effectively address IT governance principles, from a senior management level, an integrated framework is needed which aligns business and IT and addresses all relevant control areas. The starting point of the framework requires a company to distinguish between its basic business objectives and strategic business imperatives. Since basic IT controls mostly already exist at the basic business objectives level, companies often neglect to address the additional risks they are exposed to at the strategic business imperative level. It is at this level that the risk of non-alignment between IT and company objectives lies, and not at the basic business objective level, due to the fact that it is the business imperatives and not the basic business objectives that steer the vision and direction of any company. The differences between these two concepts are explained below.

Basic business objectives and business imperatives

In order for a company to successfully operate its business in a competitive environment, business objectives should be set. Two different levels of objectives are applicable, namely a company's basic business objectives and its strategic business objectives, also referred to as its business imperatives.

The first level of objectives to be set by a company relate to how the business' operations will be managed. These objectives are referred to as the company's basic business objectives. Without these objectives, no business would be able to perform its basic everyday functions effectively and efficiently in its business environment. Examples of basic business objectives include establishing a profit-orientated focus, good internal and accounting controls and standards and business continuity policies and procedures (Boshoff, 2010).

In most businesses, adequate basic IT controls are in place to address the risks occurring at the basic business objective level. However, a company's objectives do not only exist at basic operational levels, but also at a strategic level, known as a company's business imperatives. Business imperatives are those objectives, selected at a strategic level, that are the critical and fundamental business drivers which are necessary for a company to achieve its stated objectives and which give the organisation its competitive advantage in its specific environment (Boshoff, 2010). Business imperatives are specific to each business, based on the specific industry, company size, business strategies and degree of IT dependency (ITGI, 2008b).

All business areas do not carry the same IT risk profile, therefore the appropriate IT controls should be tailored to each company's specific and unique business imperatives, specifically to address these areas. The business-IT alignment process will only be achieved by implementing an integrated framework, using business imperatives as the foundation.

Integrated framework

Developing an integrated framework that combines various control frameworks -models and standards in order to simplify the overall level of control, has advantages and disadvantages.

Implementing multiple best practice control framework, -model and -standard may be arduous to implement. In addition, they can be time consuming, paper intensive, require significant resources and can become a cost intensive exercise (Rudman, 2008b). However, a single integrated framework has the following benefits.

- Three internationally accepted best practice standards are combined, which results in an integrated framework which can be applied to unique and different business requirements, while still complying with all three.

- These best practices comply with regulatory and legal requirements for IT controls in privacy and financial reporting areas.

- Costs are optimised by using standardised, rather than specifically developed, approaches which make use of experts and this uses scarce IT resources.

- There is greater control over the infrastructure, resulting in systems being more reliable, available and predictable whilst business managers gain a greater insight into the IT processes, thereby reducing major IT risks, such as the occurrence of project failures, security breaches and failures by service providers (Hardy, 2006a; ITGI, 2007; ITGI, 2008a; Johnston, Oltsik & McKnight , 2009; NUMARA, 2009).

Frameworks

Reliable controls must be put in place to ensure that a good IT governance structure is implemented. Various frameworks, -models and standards are available. By implementing the below mentioned three control frameworks,-models and standards' processes, one is able to ensure the appropriate IT related controls are implemented, ensuring IT governance principles are adhered to. Refer to section 2 for the reasons for selecting the below mentioned control frameworks,-models and standards.

COBIT control framework

The Control Objectives for Information and related Technology (COBIT) framework is an internationally accepted best practice control framework, which provides guidance in the implementation of an IT governance framework and related IT controls, to ensure that a reliable IT system is put in place (Hardy, 2006b). The purpose of COBIT is to create generally accepted IT control objectives for day-to-day use (ITGI, 2007). It has identified 34 control objectives, organised into four domains. Each domain summarises the relevant control objectives as described below:

- **Plan and Organise:** This domain focuses on the organisational and infrastructural policies that should be implemented.

- **Acquire and Implement:** This area focuses on how to identify a company's IT requirements, as well as on acquiring and implementing the required technology. It also addresses the development of an IT maintenance plan.

- **Deliver and Support:** This area focuses on the service delivery aspects of IT, including the security, support and training issues.

- **Monitor and Evaluate:** This domain assesses the effectiveness of the IT system by measuring its ability to meet business objectives and ensuring the company's control objectives comply with the requirements of internal and external auditors as well as with the relevant laws and regulations standards (Sahibudin *et al.*, 2008; Rudman, 2008a).

ITIL control model

The quality of IT services will determine the quality of the collection, analysis, production and distribution of information. Good IT service management system can be implemented by using the ITIL control model.

ITIL is a control model that describes best practices in the IT service management areas. It provides a model which addresses IT governance principles, aligns business and IT objectives, and describes the management of IT infrastructure assets, operations, development and review concepts. It also focuses on the continual measurement and improvement of the quality of IT services delivered, from both a business and a customer perspective thereby ensuring objectives are met (Cartlidge, Hanna, Rudd, Macfarlane, Windebank & Rance, 2007; Hill & Turbitt, 2006). The ITIL framework consists of the following five categories:

- **Service strategy:** This provides guidance on how to develop and implement service management principles, and how to transform such principles into strategic assets.

- **Service design:** This area focuses on the design of effective IT services which include the architecture, processes, policies and documentation design elements, in order to meet the business' requirements.

- **Service transition:** This area focuses on developing and improving transitioning capabilities, so as to convert new and changed services into operational use, ensuring that the application continue to function in the case of failures or errors occurring.

- **Service operation:** The purpose of this area is to deliver the agreed level of services to users, by managing the infrastructure, applications and the technology.

- **Continual service improvement:** This area provides guidance in maintaining and continuously improving the quality of services delivered to customers through better design, introduction and operation of services (Cartlidge *et al.,* 2007; Sahibudin *et al.,* 2008).

ISO 27001 and ISO 27002

Information has become a company's most important asset and should be protected. Accurate, reliable and timely information is needed to ensure the effective and efficient decision making. The ISO 27001 and ISO 27002 standards emphasise the importance of risk management policies and procedures, specifically relating to information security (Carlson, 2008).

The ISO 27001 standard supports the implementation of the ISO 27002 standard, since the ISO 27001 forms the foundation of the risk assessment process, governing the management controls surrounding the design, implementation, monitoring, maintenance, continuous improvements, and the certification of the information security management system (ISMS), whilst the ISO 27002 standard refers to the actual information security controls which are implemented. The following areas of controls form the basis of the ISO 27002 standard.

- **Organisational and human resource management:** These areas focus on the control environment set and communicated by management, establishing the roles and responsibilities of internal and external parties, as well as developing human resource policies.

- **Asset and physical security management:** Responsibilities should be allocated regarding the locations and ownership of assets, as well as the protection thereof against physical and environmental threats.

- **Operations management:** IT systems, networks and operational processing areas, including the control of all interactions between internal and third parties need to be managed.

- **Access controls:** Access to information should be managed at the user, network, operating systems and application level.

- **Information systems' development management:** Controls should be implemented in terms of the building, acquisition, testing, implementation and maintenance of the IT systems.

- **Incident and business continuity management:** Controls should be implemented to identify, respond, manage and recover from security incidents.

- **Compliance management:** Policies and procedures should be put in place which will ensure that the company complies with the relevant laws and regulations, security standards and audit considerations (Carlson, 2008; ITGI, 2006).

Findings

Overview of the integrated framework

In order for senior management to effectively address IT governance principles and also address all key strategic areas in a business, a model must be developed which aligns a business key strategic areas with the relevant control areas. At a strategic level, companies are driven by their business imperatives. Therefore, in order to implement strong IT governance principles, the company's strategic business objectives (known as business imperatives) must be used as its foundation, with the assumption that the basic operational day-to-day objectives (known as basic business objectives) are already in place. The control objectives of the COBIT control framework need to be aligned to the chosen business imperatives. The risks relating to the business imperatives must be identified and evaluated and the relevant COBIT control objectives identified to mitigate these risks. This creates strategic focus in the selection of the controls which are to be implemented. There is therefore no need to align and implement all (risk specific and non-specific) controls in a company. This approach recognises the fact that certain areas within a company carry a greater risk than others, and that a company does not carry one generic risk profile, as a whole.

Thereafter the relevant control objectives of the ITIL control model and the ISO 27001 and ISO 27002 standards are aligned to the relevant control objectives identified in the COBIT control framework. In light of the fact that COBIT is high-level, this mapping makes the areas of control more specific. By implementing the applicable processes of this control framework, -model and standard above, good IT governance controls can be addressed at a strategic level.

The integrated framework, shown in Figure 1, depicts the different areas which are affected and are fundamental in establishing such a framework which, when implemented, incorporates relevant control objectives needed to address the relevant risk areas. In addressing these relevant risk areas, alignment with IT governance principles are also achieved.

In order to make the framework practical and executable for senior management, it is necessary to combine all the control objectives in COBIT, ITIL and ISO 27001 and ISO 27002 to identify common control areas where these three overlap. These are mapped to business imperatives.

Determine the company's business imperatives

The foundation of implementing this framework commences with selecting the business imperatives which are applicable to a specific business environment and which can create a competitive advantage for a company. Based on a review of various literature the following 12 generalised business imperatives applicable to most businesses were identified:

- **Customer service:** through which company's can ensure that their customer service levels are superior to those of their competitors. By gathering and analysing information, companies obtain the necessary knowledge about customers' requests and products/service perceptions. By addressing these areas effectively, customers' satisfaction levels are maintained and improved (Jive Software Company, 2010; Smit, 2009).

- **Innovation:** In industries where companies are closely competitive in nature and its products only have incremental differences between them, companies constantly have to develop new products, in order to address customers' changing needs, retain their loyalty and achieve the competitive advantage. (Boshoff, 2010; Jive Software Company, 2010; Smit, 2009).

- **Affordability:** Low-cost products remain popular in meeting most consumers' buying needs (Drury, 2004). In certain companies an accurate costing system is critical to ensure that manufacturing costs are controlled and managed, determining pinpoint breakeven scenarios and improving product quality (Boshoff, 2010; Smit, 2009).

- **Diverse products or business lines:** An information system should be flexible and adaptable enough in order to incorporate diverse product lines, handling each area's costing calculations and production information accurately, and reporting on it in a timely manner. The system should also be able to deal with unique and non-standard business scenarios and an e-commerce sales environment (Boshoff, 2010).

- **Ease of use and low level of skills required:** Simple workflows and user-friendly interfaces must be implemented at workstations and in e-commerce systems, thus requiring lower skills levels from employees, end users and/or actual customers in operating the systems. This will improve the efficiency and effectiveness in which transactions and processes are handled (Boshoff, 2010).

- **Regulatory compliance:** The need to comply with the relevant laws and regulations applicable to certain companies in specific industry segments could be a critical imperative to certain companies. For example, the control and protection of sensitive information, ensuring its confidentiality, accuracy and integrity is an important imperative in highly regulated sectors, such as financial service companies, governmental institutions and national security departments (Boshoff, 2010).

- **Mobility:** Mobile access by customers to a company's product, services and information has become an important advantage in almost all businesses. Numerous applications and connectivity links should be put in place, enabling users to access secure data from, for example, virtual private networks (VPNs), and/or gain mobile access via mobile phones and 'hotspot' connections (Boshoff, 2010).

- **Reliability:** The system is required to have little or no downtime, so that users are able to rely on the system and its information. Back-up systems should also be set up in a redundancy environment (Boshoff, 2010).

- **Pro-active management:** Access to real time information and its integrated applications is a necessity when obtaining and analysing customer, financial and other information in order to make accurate and informed decisions (Smit, 2009). Information can be obtained from data resources such as data mining, enterprise resource planning (ERP) systems (Smit, 2009), blogs and social networks (Jive Software Company, 2010).

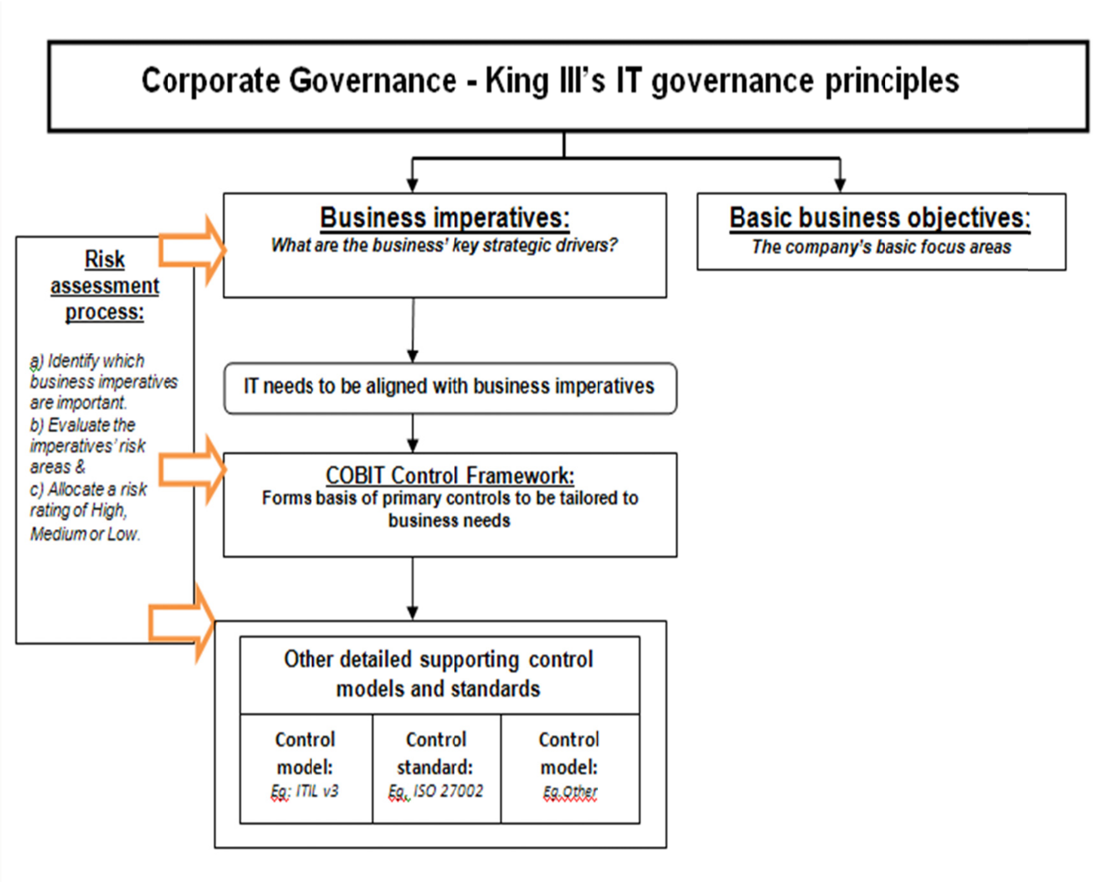
Corporate Governance - King III's IT governance principles
Business imperatives:
What are the business' key strategic drivers?
Basic business objectives:
The company's basic focus areas
Risk assessment process:
a) Identify which business imperatives are important.
b) Evaluate the imperatives' risk areas &
c) Allocate a risk rating of High, Medium or Low.
IT needs to be aligned with business imperatives
COBIT Control Framework:
Forms basis of primary controls to be tailored to business needs
Other detailed supporting control models and standards
Control model:
Eg: ITIL v3
Control standard:
Eg. ISO 27002
Control model:
Eg.Other

Figure 1: An integrated framework to align business imperatives with King III's IT governance principles at a strategic level

- **Collaboration and enterprise application integration (EAI):** Collaboration refers to the sharing of information and knowledge at an integrated level, between a company and its:

  - Suppliers and production teams, through implementing "Supply Chain Management (SCM)" systems,

  - Customers, through a "Customer Relationship Management (CRM)" system, and

  - Employees and management at various locations, different staff levels and at interrelated companies.

  -

EAI enables an enterprise to manage relationships among multiple applications and the surrounding networks or transactions (Cherry Tree & Company, 2000).

- **Productivity:** The cycle times of production processes and workflow applications should be improving on a continual basis. A reliable IT system should monitor the time spent on each activity, identifying and reporting on inefficient activities. The individual elements of the value chain should be coordinated and closely monitored in order to increase customer satisfaction and manage costs efficiently at each stage. The ultimate aim is to manage these links better than competitors do (Drury, 2004; Smit, 2009).

- **Distributed processes or replication:** Businesses which are global or multi-store orientated should have scalable or portable IT systems in place. The application systems should be designed in an uniform manner, being implemented at multi-location stores as a replica of the original version. This will also standardise the corresponding training of employees (Boshoff, 2010).

In identifying business imperatives, a company will only select the most relevant business imperatives, applicable to their business.

Once the applicable business imperatives have been selected, the next step will be to map these business imperatives to the processes of the COBIT control framework, ITIL control model and ISO 27001 and ISO 27002 control standards. It should however be noted that a company should still give consideration to the basic business objectives, which is assumed to be already in place and does not form the focus point of this article.

Key control areas covered in implementing the integrated framework at a strategic level

As discussed in section 4.2, the relevant COBIT, ITIL and ISO 27002 control objectives were combined (known as 'control areas') and summarised into seventeen possible key control areas which could be applicable in order to address IT governance principles at a strategic level.

1. **Determine business policies and strategies:** Senior management's commitment, direction and strategic objectives for the company should be documented, as well as communicated to the rest of the company. This includes implementing policies and procedures with regards to the company's internal organisational structure and external third party agreements which must be put in place.

2. **Implement business-IT alignment procedures:** IT objectives must be aligned to business objectives, resources and processes, thereby ensuring that IT delivers value to the business.

3. **Service level management procedures:** Service levels should be continuously monitored, so as to increase customer satisfaction levels. This can be achieved by implementing IT service quality reviews, reporting incidents and taking corrective actions, as well as managing the configured items and IT infrastructure components. The extent of IT resources and service levels required should be based on meeting the needs of users, and ensuring that the business strategies are achieved.

4. **Implement accurate IT resource management:** The IT architecture and technological direction of the company should be established by determining the current and future capacity of IT resources, based on a company's business requirements, identified risks, technological and economic feasibility. The IT architecture's appropriate design, development and acquisition standards should be implemented, while complying with the relevant technical requirements and the correct configuration levels. This includes the hardware, software and network architecture domains. An IT process framework should be implemented by defining the IT processes and controls at operational, organisational and technological levels, as well as assigning the appropriate IT resources to each area and IT user, based on their specific access rights.

5. **Procurement management:** A formal procurement policy should be established so as to acquire the desired level of supplier services and standard of IT resources. The agreed-upon responsibilities of suppliers will be monitored through the setting up of agreements.

6. **Access controls/ security management:** Network security controls should be established by implementing the necessary firewalls, controlling mobile code and computing, monitoring e-commerce environments, as well as controlling the network connections and access paths via configuration controls and other applicable monitoring controls. Physical access controls, including transfer controls, should be implemented in order to protect IT assets against physical and environmental hazards. An accurate inventory system should also record assets' location and ownership. It is vital to implement the appropriate information, operation and application controls, by providing the appropriate users with the correct level of access to assets and information. Rights and access should be restricted to authorised users only.

7. **The acquisition and development of an information system and maintenance controls:** Automated and manual access controls should be implemented in all stages of development or acquisition procedures. Access to the system files and the development project and supporting environments should also be controlled. Ensure data input, processing and output validation controls are in place, including cryptographic and message authentication controls. Technically vulnerable areas should also be identified and rectified.

8. **Project management:** Prioritise and coordinate projects by determining the list of deliverables, allocating accurate resources, performing a quality review of each project phase, implementing a formal test plan and performing a post implementation review of the project.

9. **Implement an information management system:** Data (both financial and operational) and integrity management controls should be implemented in order to ensure data retains its integrity, accuracy, confidentiality, availability, authenticity and non-repudiation criteria. In order to ensure quality decision making processes are possible, the right people should be provided with the right information at the right time, by implementing a quality management system. Sensitive information should be classified for security purposes, as well as implementing controls to protect documents and computer media which contain such sensitive information. Strong controls should also be implemented in data exchange situations, whether in physical or electronic form.

10. **Financial management:** The financial value of the IT assets invested and their return on investment should be monitored, as well as identifying, allocating and linking the IT assets' costs to specific users and processes.

11. **Risk management process:** A business risk impact analysis should be performed with regards to the service designs, actual services delivered and IT

process levels. An IT security plan should be implemented to address such identified risks.

12. **Change, release and deployment management**: All changes made to the system, procedures, policies, processes and configuration settings should adhere to a set control standard. These standards will include the logging, assessing and authorising of the changes to be made. A pre- and post-implementation review should be conducted on the changes implemented. Only authorised, tested and accredited components should be implemented.

13. **Human resource security:** The appropriate level of staff should be appointed, with the assistance of pre-employment screenings, adequate job descriptions, establishing employment terms and conditions, and monitoring the performances delivered. IT training should be provided to all users of IT systems.

14. **Problem management**: A reliable centralised service desk function should be established, through which all problems and security incidents can be directed, reported and resolved. The appropriate level of expertise in managing and maintaining the technical infrastructure and software applications of the systems involved should also be implemented.

15. **Business continuity management:** An IT disaster recovery plan should be developed including the establishment of off-site back-up facilities. These continuity plans should also be documented and tested on a regular basis. Controls should also be implemented to ensure the on-going recovery and capability of IT services to match the business' needs. These controls should be implemented on a continuous basis in order to remain aligned with the business' continuity plans.

16. **Compliance requirements:** Controls should be implemented so as to adhere to relevant laws and regulations, security policies, technical compliance standards and audit considerations.

17. **Configuration management:** Strong IT controls should be implemented so as to ensure that the configuration settings of IT assets are correct, authorised and that all exceptions are corrected.

Table 1 shows the mapping of the applicable key control areas which should be implemented in order to address the business imperatives' specific risk areas and thereby ensure the effective and efficient addressing of IT governance principles at a strategic level. A company deciding to address specific business imperatives would need to implement the controls around the affected areas as highlighted by an "□".

Conclusion

Senior management have been given the responsibility for addressing IT governance principles, but in most cases lack the knowledge to do so effectively. The purpose of this study is to provide a practical executable solution for the problem areas which senior management are confronted with, when attempting to address IT governance principles. One of which being the alignment of IT objectives with business objectives. Rather than reviewing and implementing multiple frameworks or models of a generic nature, a company should identify those specific business imperatives which are applicable to its business. These business imperatives should form the foundation of implementing IT governance principles at a strategic level. One of two methods can thereafter be followed by senior management in order to effectively and efficiently address IT governance principles:

i) Senior management could identify the relevant control objectives of relevant frameworks-, -models and –standards, aligning the appropriate control areas to its business imperatives. However using multiple control frameworks-, -models and –standards can become time consuming and resource intensive.

ii) This research presents a tool (in table 1) which combines three generally accepted and used control frameworks-, -models and –standards into an integrated framework which is linked to a list of generic business imperatives which can be tailored to any business. Senior management can use Table 1 to determine which *high level* key control areas need to be addressed in order to mitigate the risks associated with the specific business imperatives, most relevant to its business.

In this manner, the appropriate level of IT controls is implemented, addressing all the relevant risk areas at a strategic level applicable to a specific business, as well as addressing IT governance principles. Senior management has now been provided with a basis from which guidance and direction can be given to management at the tactical and operational levels. The next stage would entail implementing these concepts in detail at the operational level. This forms the basis of further research currently being conducted.

Table 1 – Results of the integrated framework: The key control areas which are addressed in combining and aligning the COBIT control framework, ITIL control model and ISO 27002 standard's control objectives to the relevant business imperatives

Control areas addressed:	Business imperatives											
	Innovation	Affordability	Diverse products/ Lines	Ease of use	Regulatory compliance	Mobility	Reliability	Pro-active management	Collaboration	Productivity	Customer service	Replication
1. Determine business policies and strategies	□	□	□	□	□	□	□	□	□	□	□	□
2. Implement business IT alignment procedures	□	□	□	□	□	□	□	□	□	□	□	□
3. Service level management	□	□	□	□	□	□	□	□	□	□	□	□
4. Implement IT resource management	□	□	□	□	□	□	□	□	□	□	□	□
5. Procurement management	□	□	□	□	■	□	□	■	□	□	□	□
6. Access controls/ Security management	□	□	□	□	□	□	□	□	□	□	□	□
7. Information system's acquisition, development & maintenance	□	□	□	□	□	□	□	□	□	□	□	□
8. Project management	□	■	□	■	■	■	■	■	■	■	■	□
9. Information management	□	□	□	□	□	□	□	□	□	□	□	□
10. Financial management	□	□	□	■	■	■	■	□	■	□	□	□
11. Risk management	□	□	□		□	□	□	□	□	□	□	□
12. Change, release and deployment management	□	□	□	□	□	□	□	□	■	□	■	□
13. Human resource security	□	□	□	□	□	□	□	□	□	□	□	□
14. Problem management	□	□	□	□	□	□	□	□	□	□	□	□
15. Business continuity management	■	■	■	■	□	□	□	□	□	□	□	□
16. Compliance requirements	□	■	■	■	□	□	□	□	□	■	□	■
17. Configuration management	□	■	□	□	□	□	□	□	□	■	■	□

REFERENCES

Bakari, J.K., Tarimo, C.N., Yngström, l., Magnusson, C. & Kowalski, S. 2007. 'Bridging the gap between general management and technicians – A case study on ICT security in a developing country', *Computers & Security,* **26**: 44-55.

Bleinstein, S.J., Cox, K., Verner, J. & Phalp, K.T. 2005. 'B-SCP: A requirements analysis framework for validating strategic alignment of organizational IT based on strategy, context, and process', *Information and Software Technology,* **48**: 846-868.

Boshoff, W.H. 2010. Masters in accounting (computer auditing). Unpublished lecture slides. Stellenbosch: University of Stellenbosch.

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.

Carlson, T. 2008. ‘Understanding ISO 27002'. [online] URL: http://www.orangeparachute.com/documents/Understanding_ISO_27002.pdf.

Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I., Windebank, J. & Rance, S. 2007. ‘An introductory overview of ITIL V3.' [online] URL:http://www.itsmfi.org/files/itSMF_ITILV3_Intro_Overview_0.pdf.

Cherry Tree & Company. 2000. ‘Extended enterprise applications'. [*o*nline] URL:http://www.sysedv.tu-berlin.de/intranet/kc-kb.nsf/bc64cc33c3daf5fec1256979005bc026/F16DB8D8AA21A63DC1256CD300398C69/$File/Extended+Enterprise+Applications.pdf?OpenElement.

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

Doughty, K. & Grieco, F. 2005. ‘IT governance: Pass or fail'. [online] URL:http://www.isaca.org/Journal/Past-Issues/2005/Volume-2/Documents/jopdf052-IT-Gov-Pass-or-Fail.pdf.

Drury, C. 2004. *Management and cost accounting.* 6th Edition. London: Thomson Learning.

Hardy, G. 2006a. ‘Guidance on aligning COBIT, ITIL and ISO 17799'. [online] URL:http://www.isaca.org/Journal/Past-Issues/2006/Volume-1/Documents/jpdf0601-Guidance-on-Aligning.pdf.

Hardy, G. 2006b. 'Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges', *Information Security Technical Report,* **11**: 55-61.

Hill, P. & Turbitt, K. 2006. ‘Combine ITIL and COBIT to meet business challenges'. [online] URL:http://www.vpit.ualberta.ca/frameworks/pdf/itil_cobit.pdf.

IBM. 2006. ‘Igniting innovation through business and IT fusion'. [online] URL:http://www-935.ibm.com/services/fr/cio/flexible/flex_wp_gts_fusion_business_it.pdf.

Innotas. 2010. ‘The CXO’s guide to IT governance. A roadmap to driving top-down alignment between business & IT strategy.' [online] URL:http://solutioncenters.cio.com/innotas_governance/registration/5962.html?source=ciozne.

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

IT Governance Institute (ITGI). 2006. ‘COBIT mapping: Overview of international IT guidance'. *2nd Edition.* [online] URL:http://www.sox-expert.com/uploads/files/COBIT%20Mapping%202nd%20Edition.pdf .

IT Governance Institute (ITGI). 2007. ‘COBIT 4.1'. [online] URL:http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-4-1.aspx.

IT Governance Institute (ITGI). 2008a. ‘Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for business benefit.' [online] URL:http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT,ITILV3,ISO27002-Bus-Benefit-12Nov08-Research.pdf.

IT Governance Institute (ITGI). 2008b. ‘COBIT mapping. mapping of ITIL v3 with COBIT 4.1.' [online] URL:http://www.itsm.hr/baza%20znanja/Mapping%20ITILV3%20COBIT41.pdf.

IT Governance Institute (ITGI). 2008c. ‘Understanding how business goals drive IT goals'. [online] URL:http://www.isaca.org/Knowledge-Center/Research/Documents/Understand-Bus-Drive-IT-Goals-15Oct08-Research.pdf.

Jive Software Company. 2010. ‘The 18 social business imperatives'. [online] URL: http://www.jivesoftware.com/files/pdf/whitepaper/WP-18BusinessImperatives-JiveSoftware.pdf.

Johnston Turner, M., Oltsik, J. & McKnight, J. 2009. ‘ISO, ITIL & COBIT together foster optimal security investment'. [online] URL: http://www.thecomplianceauthority.com/iso-itil-a-cobit.php.

Kordel, L. 2004. ‘IT governance hands-on: Using CobiT to implement IT governance'. [online] URL:http://www.isaca.org/Journal/Past-Issues/2004/Volume-2/Documents/jpdf042-ITGovernanceHands-on.pdf

Liell-Cock, S., Graham, J. & Hill, P. 2009. ‘IT governance aligned to King II*I'*. [online] URL:http://lgict.org.za/sites/lgict.org.za/files/documents/2009/liell-cock-graham-hill-2009-it-governance-aligned-king-iii.pdf.

Muller, R. 2009. ‘IT governance report slated'. [online] URL:http://mybroadband.co.za/news/general/7242-it-governance-report-slated.html.

Numara Software. 2009. ‘Show me the money. How life in the ITIL fast lane can deliver success'. [online] URL: http://www.findwhitepapers.com/whitepaper7394.

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

Rudman, R.J. 2011. 'IT governance failure', *Auditing SA*. **Summer** 2010/2011:37 – 39.

Rudman, R. J. 2010. 'Framework to identify and manage risks in web 2.0 applications', *African Journal of Business Management,* **4**(13): 3251 – 3264.

Rudman, R.J. 2008a. 'Demystifying COBIT'. [online] URL:http://www.accountancysa.org.za/resources/ShowItemArticle.asp?ArticleId=1398&Issue=979.

Rudman, R.J. 2008b. 'IT governance: A new era', *Accountancy SA*, **March** : 12 – 14.

Sahibudin, S., Sharifi, M. & Masarat, A. 2008. 'Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations'. [online] URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4530569 .

Smit, S. 2009. 'Defining and reducing the IT gap by means of comprehensive alignment'. Unpublished master's thesis. Stellenbosch: University of Stellenbosch.

Steenkamp, G. 2011. 'The applicability of using COBIT as a framework to achieve compliance with the King III Report's requirements for good IT governance', *Southern African Journal of Accountability and Auditing Research,* **11**:1-8.

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

Voogt, T. 2010. 'IT governance, Dear CFO, what should you do?' [online] URL:http://www.accountancysa.org.za/resources/ShowItemArticle.asp?ArticleId=2044&Issue=1097.