

# An Integrated Framework To Implement IT Governance Principles At A Strategic And Operational Level For Medium-To Large-Sized South African Businesses

Riana Goosen, Stellenbosch University, South Africa  
Riaan Rudman, Stellenbosch University, South Africa

## ABSTRACT

*In today's technologically advanced business environments, Information Technology (IT) has become the center of most, if not all, business activities; consequently, the King III report in South Africa dedicated a chapter to IT governance principles, making senior management responsible for implementing such principles. The King III's implementation guidance lacks detail as to how to implement its principles. Although various guidelines in the form of IT control frameworks - models and standards - exist, it remains theoretical in nature. Companies tend to view these control frameworks on an individual basis, implementing them in an ad hoc manner, resulting in the implementation of an inefficient IT governance system that either addresses strategic areas, but not operational areas, of a business or vice versa.*

*The purpose of this study is to develop an IT best practices integrated framework that can assist management in implementing an effective IT governance system at both a strategic and operational level. The integrated framework was developed by performing a detailed literature review of selected best practice control frameworks and its underlying processes. By combining the relevant processes of the control frameworks and aligning them to general business' imperatives, IT governance principles can be implemented at a strategic level. By identifying and linking the relevant business imperatives and control areas to the access paths of an IT system, IT governance principles can be implemented at an operational level. By making use of the integrated framework, an IT governance system can be implemented at both a strategic and operational level.*

**Keywords:** IT Governance; Strategic Level; Operational Level; Control Frameworks; King III Report

## 1. INTRODUCTION AND BACKGROUND

 Effective corporate governance principles form the foundation of any successfully managed business. For the past two decades, the King reports have formed the basis for the implementation of good corporate governance practices in South African companies. The third King report emphasised the implementation of strong information technology (IT) governance principles for the first time (IODSA, 2009). The rationale for including IT governance matters in the King report is emphasised by the changing nature of businesses' IT environments, which include inter alia-extended enterprises, cloud computing, and collaboration elements. IT has become an integral part of the day-to-day operations of any business (IODSA, 2009) as well as being part of the strategic planning process. This poses a challenge to senior management, and directors specifically, with regard to how to practically implement these IT governance requirements that appear vague, unclear (Muller, 2009), and are only addressed at a high-level. A number of best practice IT control frameworks are available to develop and implement a high quality IT governance system through which business and IT management are required to work together on its implementation. However, these two management groups address either strategic concepts or

technical concepts, respectively. The two groups are responsible for implementing IT principles with a different understanding of the required control frameworks (Rudman, 2011). This results in a misalignment between IT objectives and a company's business objectives, known as the 'IT gap'. This gap is further widened by IT management who attempts to implement IT controls without effectively understanding and addressing the business' IT risk areas. This results in the implementation of an ineffective IT governance system (Rudman, 2010). In order to overcome this gap and the *ad hoc* implementation of controls, a business needs to implement an integrated framework (as developed in this article) which can bridge the IT gap between the implementers of IT governance principles at both a strategic and operational level, as well as implementing effective and efficient alignment of the business to IT objectives. Business and IT management are required to work together in implementing such a system.

Research on establishing effective IT governance and business-IT alignment has been documented by various researchers, as discussed below, but has not been addressed in an integrated manner. 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 various control guidelines and frameworks, such as the Committee of Sponsoring Organisations of the Treadway Commission's (COSO) framework, the Projects in Controlled Environments (PRINCE II) project management methodology, and the Code of Practice for Information Security Management (ISO 27002) standard (ITGI, 2006).

In 2008, the ITGI performed further mapping between the control objectives of the IT best practice control frameworks COBIT, the Information Technology Infrastructure Library (ITIL), and ISO 27002 (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, and an attempt was made to align generic strategic business objectives with the COBIT's control framework processes. Steenkamp (2011) and Hardy (2006b) showed that by implementing COBIT's control objectives, a business 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.

These studies focus 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 and only deal with selected aspects of the IT governance alignment process and do not address these aspects in an integrated manner. Moreover, the link to implementation at an operational level has not been made.

### **1.1. Research Objective And Motivation**

Guidance on IT governance matters and IT risk management that impacts a business at a strategic and operational level is not readily available to board of directors and senior management (Hardy, 2006b). This article proposes to address this lack of guidance available relating to the implementation of IT governance principles provided by the King III report by developing a practical integrated framework that addresses IT governance at both a strategic and operational level and which links these two levels. It is the purpose of this research to develop a framework that 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 at a strategic level whilst aligning IT and business management's understanding of the business objectives. There are three secondary research questions: 1) How do you implement IT governance at a strategic level?, 2) How do you implement IT governance at an operational level, and 3) How do you bridge the IT gap.

This framework will provide management with a tool that can be used to implement such principles at a strategic and operational level by aligning the control objectives of various IT control frameworks to a business' unique strategic objectives and relating them to the components underlying the technology that makes up an organisation's IT system. This practical integrated framework will allow business and IT management to address the key IT risks as well as strategic areas at the same time. It will provide management with a tool to understand the technical and strategic IT aspects of an IT system. It will also help non-IT management to ask the right questions

when considering the operational implications of IT.

Since every business' strategic 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 that 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 and not governance principles, in general. The findings are 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.

## **1.2. 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 and operational level. An overview of the research, highlighting the outcomes of the research findings and discussing the practical implementation of the integrated framework, is contained in Section 5.

## **2. RESEARCH METHODOLOGY**

In order to fully implement IT governance, a framework is necessary that links strategic aspects with operational aspects. IT governance principles are addressed by identifying a business' strategic objectives (hereafter referred to as a company's 'business imperatives') and implementation of the relevant control objectives, which can be tailored to any business using either an IT control framework or a combination thereof. In order to develop this integrated framework, the following process was used.

A literature review was performed in order to obtain an understanding of the concept of business imperatives as well as various control frameworks. Based on the literature review, the COBIT, ITIL and ISO 27002 (supported by ISO 27001) control frameworks 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 performs a high-level risk assessment on the general control environment. The ITIL control framework identifies operational risks and provides guidance on how to effectively implement service management principles, whilst the ISO 27001 and ISO 27002 control frameworks address the information security risk matters (Sahibudin, Sharifi & Masarat, 2008). Given the level of detail of these control frameworks, this study was limited to identifying internal controls as defined by COSO's definition of an internal control. These three control frameworks 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).

The relevant strategic business imperatives relevant to most businesses were identified from literature. These imperatives were hereafter mapped to each control area to form the basis of the implementable integrated framework in the form of a matrix. This matrix provides the basis for implementation of IT governance principles at a strategic level.

Based on the selected business imperatives, IT governance controls are also to be implemented at an operational level. The implementation of IT governance principles at an operational level was achieved by:

- performing a detailed literature study of the selected frameworks in order to identify the detailed control techniques (actual controls to be implemented at the operational level)
- further extending the literature review to better understand and define the concept of access paths as well as the different components of each access path
- conducting a high-level investigation on the risks surrounding access path components and methods in which such risks can be managed by implementing appropriate configuration controls

By following the above-mentioned methodology, a framework was developed to ensure compliance with IT governance principles, at both a strategic and operational level, and thereby addressing the problem created by the ‘IT gap’.

### **3. LITERATURE REVIEW**

In order to understand how an IT governance system can be implemented, it is necessary to understand the context and environment in which IT operates, as well as its related constraints. The following sections outlines the theoretical concepts underlying governance and, in particular, IT governance. It also outlines why it is important to implement frameworks.

#### **3.1. Corporate And IT Governance**

Corporate governance can be viewed as the overall business structure and ethical values which determine a business’ direction and performance standards. The board of directors, senior management, shareholders, employees, and any other related parties are responsible for implementing good corporate governance policies to ensure that appropriate controls (manual or electronic) are in place, creating a strong control environment which ensures that ethical, accountable, fair, transparent, and reliable actions are performed by all parties (IODSA, 2009). This control environment includes IT systems. The King III report recommends that directors should 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 business’ specific requirements, in order to ensure that a business achieves its strategic objectives (IODSA, 2009).

Since IT has become the centre of many business activity and has an impact on both strategic and operational levels, IT should ensure reliable sources of information (Voogt, 2010), which are free from fraud and error (Hardy, 2006b). IT strategies, policies, budgets and good IT investment returns will only be obtained when good IT governance practices are implemented (Voogt, 2010). Section 5 of the King III report (IODSA, 2009) highlights seven key IT governance principles that must be implemented:

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 expenditures.
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.

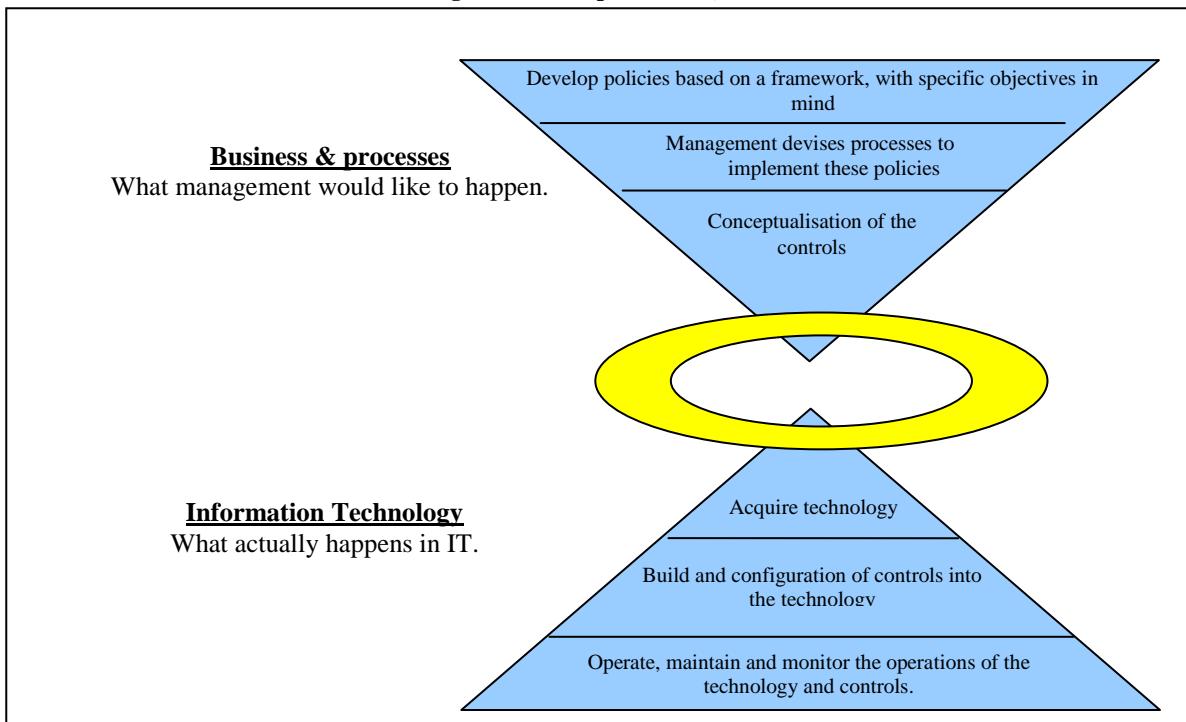
If these principles are addressed in the IT system, it can be expected that a business’ reputation will improve and that trust between internal parties (such as employees) and external parties (such as customers, suppliers and investors) will improve. It will also help prevent fraudulent activities, which can lead to civil and criminal liabilities (Olivier, 2012). Strong IT governance practices create a competitive advantage by strategically aligning IT with business goals and processes, making business operations more efficient and effective, whilst non-IT executives gain a better understanding of IT and better decision-making processes are possible due to timely and quality information being available. A greater level of compliance with laws and regulations is also possible and risk management procedures are maximised by implementing good IT controls (Bowen, Cheung & Rohde, 2007; Hardy, 2006b).

If good IT governance practices are not implemented, the business’ operational risk increases as well as a risk of loss of confidentiality, integrity, and authenticity of information systems. IT systems can become less available, less reliable, and function less effectively whilst unauthorised use, access, and changes to IT systems also become a greater risk (IODSA, 2009). In order to realise these benefits and mitigate these issues, certain problem areas need to be addressed; namely, the ‘IT gap’ and business-IT alignment areas. Once these problem areas have been adequately addressed, the guidance provided in the integrated framework can be implemented, resulting in the implementation of an effective and efficient IT governance system.

### 3.2. ‘IT Gap’ And Business-IT Misalignment

During the implementation of the IT governance principles (mentioned in Section 3.1.) miscommunication between the senior management of a business (responsible for ensuring sufficient and effective internal control systems) and IT specialists (responsible for implementing such controls) inevitably occurs. This creates a problem as top management does not understand the IT control techniques (the actual controls implemented to address the identified risks) and technology, whereas IT specialists do not understand the control frameworks (a system that covers all fundamental internal controls expected to mitigate the risks as well as 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’ disparity and is depicted in Figure 1.

**Figure 1: IT Gap (Rudman, 2008b)**



The IT gap exists due to business managers not understanding the technological environment in which the business operates nor the extent to which IT can support the business to achieve its objectives (The Economist, 2006). This results in a misalignment between IT and business elements due to constant changes in these environments. This needs to be understood (Chen, Kazman & Garg, 2004). A misalignment exists between the objectives of the IT department and the business executives' objectives for IT (Simkova & Basl, 2006). A business-IT alignment process must be implemented in order to overcome this gap between IT and business managers' perceptions surrounding IT matters.

In order for a business to successfully achieve a business-IT alignment environment, it is important that an enterprise's strategic and business objectives be 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' objectives, the business-IT alignment process is achieved (Bleinstein, Cox, Verner & Phalp, 2005). This has the advantage that IT strategies become aligned with and are supportive of the strategic business objectives, which reduces the business and IT-related risks whilst reliable real-time data improves decision-making, which will lead 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 failing 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 could occur due to ineffective and incomplete IT controls (Smit, 2009), whilst excessively high IT costs and overheads occur due to the ineffective use of IT resources (IBM, 2006). There is also a risk of increased legal action due to the breaching of relevant laws and regulations (Bakari *et al.*, 2007).

In order to achieve business-IT alignment and effectively implement IT governance principles, a business will need to implement an integrated framework.

### **3.3. Foundation Of An Integrated Framework**

The starting point of the framework requires a business to distinguish between their basic business assumptions and business imperatives. In order for a business to successfully operate its business in a competitive environment, business objectives must be set. Two different types of objectives are applicable; namely, a company's basic business assumptions and its strategic objectives, also referred to as its business imperatives.

#### *3.3.1. Basic Business Assumptions*

A company's basic business assumptions refer to those objectives which relates to how the business' operations will be managed. Without these objectives, no business would be able to perform its everyday functions effectively and efficiently. Examples of basic business assumptions include a profit-orientated focus, good internal and accounting controls and standards, business continuity policies and procedures, and data accuracy and security matters.

Adequate basic IT controls are put in place in most businesses to address the risks occurring at the basic business assumption level. However, a business' objectives do not only exist at a basic operational level, but also at a strategic level (Boshoff, 2010).

#### *3.3.2. Business Imperatives*

Business imperatives are those objectives selected at a strategic level that are seen as the critical and fundamental business drivers that are necessary for a business to achieve its competitive advantage in its specific environment (Boshoff, 2010). Business imperatives are specific to each business based on, *inter alia*, the specific industry, business size, business strategies, and degree of IT dependency (ITGI, 2008b).

The business-IT alignment process will be achieved by implementing an integrated framework using a company's business imperatives as the foundation.

### **3.4. Frameworks**

Three internationally recognised control frameworks - COBIT, ITIL and ISO 27002 - were selected to form the basis of the integrated framework. Section 2 outlines the reasons for selecting these control frameworks.

#### *3.4.1. COBIT Control Framework*

The Control Objectives for Information and related Technology (COBIT) control framework describes which types of IT controls should be implemented in order to achieve a good IT governance structure and a reliable IT system (Hardy, 2006b). The purpose of COBIT is to create generally-accepted IT control objectives for day-to-day use (ITGI, 2007). COBIT focuses on closing the gap between business risk, control needs, and technical issues (ITGI, 2007). It has identified 34 processes organised into four domains which each summarise the relevant processes involved. Each process is linked to a control objective which can be used to design an appropriate control, activity, or task in order to address the risks identified (Rudman, 2008a). The four domains are:

- Plan and Organise - how to establish the organisational and infrastructural policies in order to optimally utilise IT resources
- Acquire and Implement - the identification of a business' IT requirements when implementing and monitoring an IT plan
- Deliver and Support - the service delivery and support aspects of IT, including the security, support, and training issues
- Monitor and Evaluate - how to effectively assess and measure the IT system's ability in meeting business objectives and complying with relevant laws and regulations (Sahibudin *et al*, 2008; Rudman, 2008a)

### *3.4.2. ITIL Control Model*

The Information Technology Infrastructure Library (ITIL) framework describes best practices in the area of IT service management, which should ensure the delivery of quality IT services by describing the management of IT infrastructure assets, operations, development, and review concepts whilst continuously measuring and improving the quality of IT services delivered from both a business and a customer perspective (Cartlidge *et al*, 2007; Hill & Turbitt, 2006). The ITIL framework focuses on five categories:

- Service Strategy - provides guidance on how to develop and implement service management principles and service strategies.
- Service Design - focuses on the design of effective IT services which include the architecture, processes, policies, and documentation design elements.
- Service Transition - focuses on developing and improving transitioning capabilities resulting in services becoming operationally faster.
- Service Operation - provides the details of managing the infrastructure, applications, and the technology aspects to ensure the delivery of services at the agreed level.
- Continual Service Improvement - provides guidance on continuously improving the quality of services through better design, introduction, and operation of services (Cartlidge *et al*, 2007; Sahibudin *et al*, 2008).

### *3.4.3. ISO 27001 And ISO 27002*

According to ISACA's (Information Systems Audit and Control Association) 2012 survey on governance of enterprise, IT data leakage was seen as the top IT issue in African and European companies with regard to network security matters (ISACA, 2012). It is therefore clear that information has become a business' most important asset and should be protected accordingly. Accurate, reliable, and timely information is needed to ensure the effective and efficient use of information in decision-making processes. ISO 27001 and ISO 27002 emphasise the importance of risk management policies and procedures specifically relating to information security (Carlson, 2008).

ISO 27001 supports the implementation of ISO 27002. These two standards are usually implemented together in order to ensure a secure information system (Wallhoff, 2004). ISO 27001 provides a high level framework for establishing the foundation of the Information Security Management System (ISMS) (Kosutic, 2010) whilst ISO 27002 refers to the actual information security operational controls (Maxi-pedia, 2011).

Once the IT strategy and the applicability of ISO 27001 have been established, it is possible to implement the actual controls as listed in ISO 27002 (Kosutic, 2010). The following areas were identified:

- Organisational And Human Resource Management - developing the control environment and policies and procedures surrounding employing, training, and terminating employees
- Asset And Physical Security Management - developing policies and procedures in terms of assigning responsibility for ownership and protection of assets (including security management)
- Operations Management - implement policies and procedures over the operating of IT systems, networks, and other operational processing areas, including the control of all interactions between internal and external parties at information exchange and service delivery levels

- Access Controls - controlling access to the information assets by managing the user, network, operating system, and application access elements
- Information Systems' Development Management - controls implemented during the building, acquisition, testing, implementation, and maintenance of the IT systems
- Incident And Business Continuity Management - identifying, responding, and managing security incidents, as well as developing an IT disaster recovery plan to ensure the continuity of operations
- Compliance Management - implementing policies and procedures to ensure compliance with the relevant laws and regulations, security standards, and audit considerations (Carlson, 2008; ITGI, 2006)

### **3.5. Integrated Framework**

The above-mentioned control frameworks address different areas and could be combined to develop the integrated framework. Implementing these multiple best practice control frameworks separately 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 frameworks are combined, which results in an integrated framework that can be customised to unique and different business requirements.
- These best practices comply with regulatory and legal requirements for IT controls in privacy and financial reporting areas.
- Costs are optimised by using a standardised - rather than specifically developed - approach which makes use of experts and 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, Olsik & McKnight, 2009; NUMARA, 2009).

By combining and aligning the processes of the above-mentioned control frameworks, the integrated framework's best practice processes can be identified which can be implemented at a strategic level. However, implementing these processes at an operational level is more challenging (as described in Section 3.2.) with regard to bridging the IT gap which will include mechanisms such as understanding access paths and configuration controls.

### **3.6. Access Paths And Configuration Controls**

When implementing IT governance principles at an operational level, it is not as easy as simply implementing control techniques for each control area. Tools, such as access paths, should be used to systematically analyse and understand the technology underlying the IT system. Implementing controls at an operational level commences with identifying the relevant access paths and evaluating the access paths' individual architectural components in the context of the relevant business imperatives. This will provide the understanding into which identified areas the relevant risks lie.

A user performs computerised activities by activating an access path. An access path is formed by the various IT components that need to be activated in order for a typical user (business, IT, or otherwise) request (functionality, data or otherwise) to be executed in order to access computer-controlled resources (Boshoff, 2010). An access path is created by joining various IT components, such as computers, laptops, operating systems, routers, switches, the internet connection, servers, and other relevant IT components. There may be multiple access paths for the same user or activity (Boshoff, 1990). Each access paths' individual IT architectural components should be identified and examined to ensure that they are correctly built, set up, configured, operated, and/or maintained in order to implement the appropriate controls in a particular access path (Boshoff, 2010). These controls are referred to as configuration controls.

Configuration controls ensure that the settings of these components are correctly determined in accordance with the stated security and compliance policies. Configuration controls detect all changes made across the IT infrastructure whether they are made to applications, databases, operating systems, directories, or network devices. They assist in detecting and reporting on every change made by any method, including circumvented and unauthorised changes, and discovering configuration errors timely in order to minimise troubleshooting matters (Santarcangelo, 2010). This also allows for a better understanding of the components and a more comprehensive approach to analysing the system. If both business and IT management understand access paths and its related configuration controls, it will bridge the IT gap at an operational level as well as result in an effective oversight of all infrastructure changes, detecting unauthorised changes and non-conforming configuration settings. Faster responses are provided to troubleshooting scenarios and less rework is needed due to fewer unplanned emergencies and unauthorised changes. Greater availability, integrity, and credibility of IT systems are also possible. Strong security measures mitigate the relevant risks by ensuring that all changes are detected, authorised, and documented, lowering compliance costs (Tripwire, 2007).

Should configuration controls not be implemented, unintentional access may be granted to unauthorised users due to, for example, incorrect web server configuration or ports accidentally left open on the external router, etc. Both a business' 'known assets' (currently 'active' assets that IT is aware of) and the 'unknown assets' (the 'inactive/passive' assets which are not active at present or which IT is unaware of) should be correctly configured over the areas such as the entire network, web, enterprise applications, middleware, databases, as well as operating systems and network infrastructures (Santarcangelo, 2010).

### **3.7. Summation Of Literature Review**

These concepts discussed form the foundation underlying an integrated framework which can overcome the 'IT gap', achieve business-IT alignment between a company's business and IT objectives, as well as implement appropriate IT controls at a strategic and operational level in order to comply with King III's IT governance requirements.

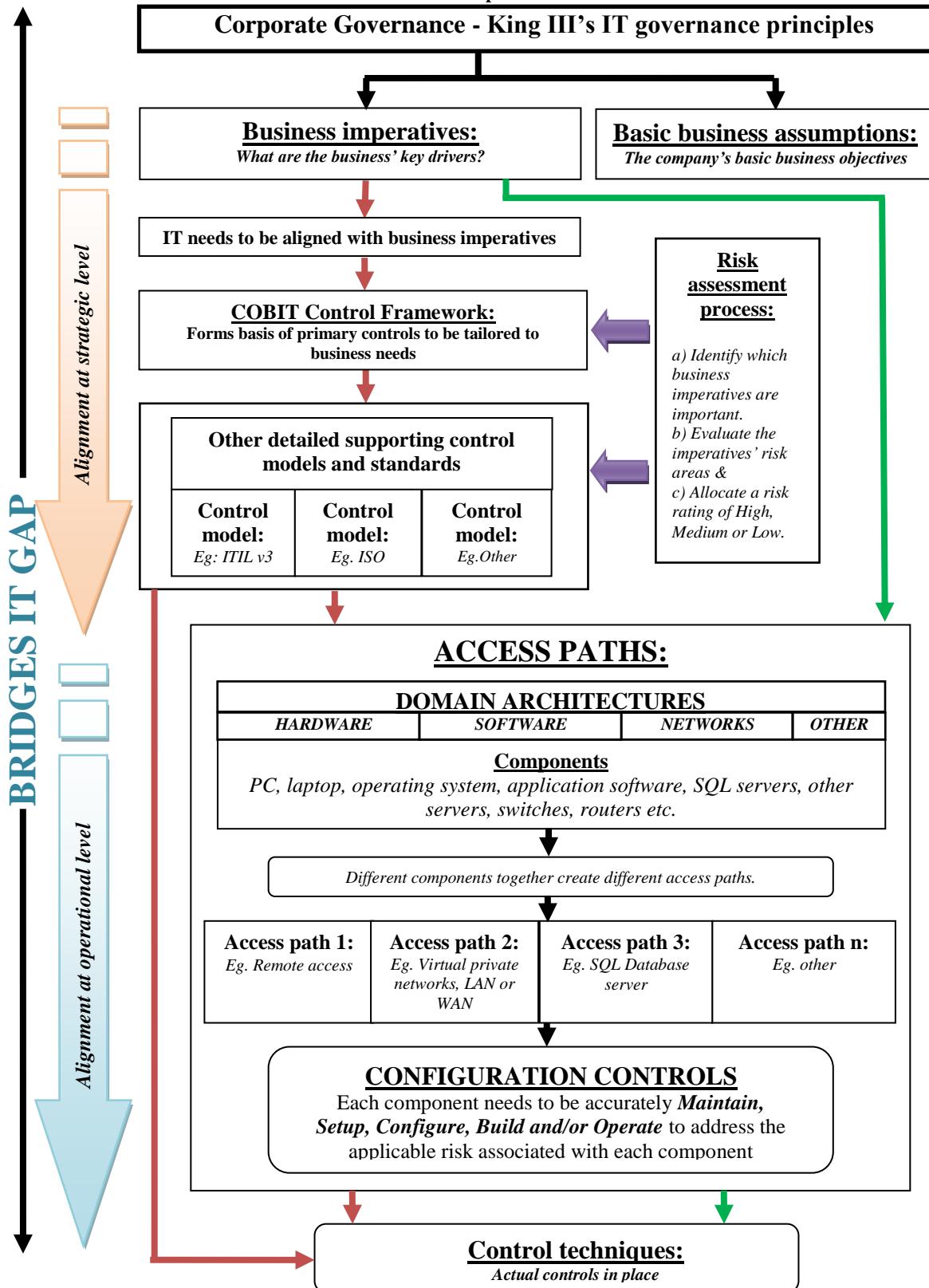
## **4. FINDINGS**

### **4.1 Overview Of The Integrated Framework**

In order to effectively implement IT governance principles at both a strategic and operational level, a framework must be developed that not only - at a strategic level - aligns a business' key focus area (business imperatives) with the relevant control areas (control processes) and - at an operational level - analyses the technology in an accurate, complete, and understandable manner, but also brings the two levels together in order to bridge the IT gap. Figure 2 depicts such a framework.

Sections 4.1.1. and 4.1.2. present a narrative explaining Figure 2 which graphically presents the integrated framework to align business imperatives with Information Technology governance principles at both strategic and operational levels.

**Figure 2: An Integrated Framework To Align Business Imperatives With Information Technology Governance Principles**



#### *4.1.1. Strategic Level*

Most management teams predominantly focus on implementing controls to address the risks of the basic business assumption areas in a company and often neglect to address the additional risks a company is exposed to at a strategic level; namely, the risks relating to the business imperative areas. Business imperatives are distinct from its basic business assumptions. At a strategic level, companies are driven by their business imperatives and should therefore form the foundation on what the framework is to be built on. This creates strategic focus in the selection of the controls that are to be implemented. Therefore, there is no need to align and implement all (risk-specific and non-specific) controls in a business. This approach recognises the fact that certain areas within a business carry a greater risk than others and that a business does not carry one generic risk profile as a whole. It is for this reason that basic business assumptions are not seen as the areas of risk due to basic controls already being implemented in these areas in most companies.

Therefore, in order to establish and implement strong IT governance principles, the company's business imperatives will be used as its foundation in developing an integrated framework. 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.

Thereafter, the relevant control objectives of the ITIL control framework and ISO 27001 and ISO 27002 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 these control frameworks, good IT governance controls can be addressed at a strategic level.

The integrated framework, shown in Figure 2, depicts the different areas that 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, ISO 27001, and ISO 27002 in order to identify and group it into similar control areas where these frameworks overlap. These can be mapped to a company's business imperatives.

#### *4.1.2. Operational Level*

At an operational level, the control frameworks' processes - identified at the strategic level (Section 4.1.1.) - need to be used to identify and implement the actual control techniques within an IT system. Access paths will be the second part that will be used to gain an understanding of the IT system. The technology making up the access paths can be classified according to either architecture or components. Access paths are also affected by the applicable business imperatives. By identifying and evaluating the risks of the access paths and by giving consideration to the relevant configuration controls and the appropriate control techniques, IT governance principles could be addressed at an operational level.

### **4.2. Implementation Guidance Of The Integrated Framework**

In order for companies to effectively and efficiently implement IT governance principles, the following elements should be considered at the strategic and operational levels.

#### *4.2.1. Steps In Implementing IT Governance At A Strategic Level*

The following steps should be followed at a strategic level:

- Determine a company's business imperatives and evaluate its importance. These imperatives need to be separated from a company's basic business assumptions.

- Evaluate the risks associated with the business imperatives and identify which COBIT processes will appropriately address these risks.
- Link the relevant ITIL and ISO 27002's control processes to the appropriate COBIT processes which, in turn, link to the specific business imperatives (refer to step 2).

This will result in the identification of the appropriate control processes most important to a business.

#### **4.2.2 Steps In Implementing IT Governance At An Operational Level**

Controls at the operational level can be identified by *both* relying on the detail contained in the individual frameworks and by means of analysing the access paths into its components and evaluating each component against the applicable business imperative and control area.

### **4.3 Implementing IT Governance Principles At A Strategic Level**

#### **4.3.1. Determine The Company's Business Imperatives**

The foundation of implementing this integrated framework commences with selecting the business imperatives that are applicable to a specific business environment. Twelve business imperatives were identified by Boshoff (2010), Drury (2004), and Smit (2009) which could be applicable to most companies and which creates a competitive advantage for a business:

- Customer Service – Companies are able to gain a competitive advantage by ensuring their customer service levels are superior to those of their competitors.
- Innovation – Companies need constant innovation in its product lines where competitor companies offer products with only incremental differences between them.
- Affordability – Companies can also achieve a competitive advantage through the sale of low-cost products in meeting a certain consumer's profile buying needs.
- Diverse Products Or Business Lines – An information system should be flexible and adaptable in order to incorporate diverse product lines, deal with unique and non-standard business scenarios and an e-commerce sales environment.
- Ease Of Use And Low Level Of Skills Required – Simple workflows and user-friendly interfaces for employees and end-users must be implemented at workstations and in e-commerce systems.
- Regulatory Compliance – The need to comply with the relevant laws and regulations, including controlling and protecting sensitive information, could be a critical imperative in highly regulated sectors.
- Mobility – Mobile access by end-users to a business' product, services and information has become an important customer requirement in today's business environment.
- Reliability – The system is required to have little or no downtime in order that users are able to rely on the system and its information.
- Pro-active Management – Analysing customer and product information in real time could be crucial in providing the necessary insight required for decision-making processes and to gain a competitive advantage in a business' industry.
- Collaboration (Enterprise Application Integration [EAI]) – A competitive advantage can be obtained by sharing information and knowledge between a business and its suppliers, production teams, customers, employees at different staff levels, and management at various locations (Cherry Tree Company, 2000).
- Productivity – The cycle times of production processes and workflow applications should improve continuously in order to improve customer satisfaction and manage costs efficiently.
- Replication – Businesses that are global or multi-store orientated should have replicas of the original version of application systems installed at the multi-location stores which will standardise the corresponding training of employees.

In identifying business imperatives, a business 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 control areas of the COBIT, ITIL, and ISO 27002's control frameworks. It should, however, be noted that a business should still give consideration to the basic business objectives, as discussed in Section 4.1.1., which is assumed to be already in place and does not form the focus of this article.

#### *4.3.2 Key Control Areas Covered In Implementing The Integrated Framework At A Strategic Level*

As discussed in Section 4.2.1., the relevant COBIT, ITIL, and ISO 27002 control objectives were combined and summarised into seventeen possible key control areas:

- Determine Business Policies And Strategies - Management's commitment, direction and strategic objectives for the business should be documented and communicated to the rest of the business.
- 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.
- Service Level Management Procedures - IT resources should be managed, prioritised, and aligned in achieving the business' strategic objectives, as well as continuously monitoring service levels to increase customer satisfaction levels.
- Implement Accurate IT Resource Management - The IT architecture and technological direction of the business 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.
- Procurement Management - A formal procurement policy should be established in order to acquire the desired level of supplier services and standard of IT resources.
- Access Controls/ Security Management - Network security controls, such as firewalls, controlling mobile code, and controlling the network connections, should be implemented, as well as the necessary physical access controls which will protect IT assets against physical and environmental hazards. The appropriate information, operation, and application controls should also be implemented.
- 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.
- 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.
- Implement An Information Management System - Data (both financial and operational) and integrity management controls should be implemented in order to ensure that data retains its integrity, accuracy, confidentiality, availability, authenticity, and non-repudiation criteria. This will ensure that a quality information management system is in place.
- Financial Management - The financial value of the IT assets invested - and their return on investment - should be monitored as well as IT asset's costs identified, allocated, and linked to specific users and processes.
- Risk Management Process - A business risk impact analysis should be performed with regard to the service designs, actual services delivered, and IT process levels. An IT security plan should be implemented to address such identified risks.
- Change, Release And Deployment Management - All changes made to the system, procedures, policies, processes, and configuration settings should adhere to a set control standard.
- Human Resource Security - The appropriate level of staff should be appointed in the correct positions as well their performances monitored. IT training should also be provided to all users of IT systems.
- Problem Management - A reliable centralised service desk function should be established through which all problems and security incidents can be directed, reported, and resolved.
- Business Continuity Management - An IT disaster recovery plan should be developed, including the establishment of off-site back-up facilities.
- Compliance Requirements - Controls should be implemented so as to adhere to relevant laws and regulations, security policies, technical compliance standards, and audit considerations.
- 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.

#### 4.3.3 Mapping Of Business Imperatives To Key Control Areas

A broad-based list of business imperatives, which could be applicable to a business environment, was identified in Section 4.3.1. In aligning the applicable business imperatives to the control processes of the selected control frameworks, key control areas were identified that will summarise which IT processes need to be implemented at a strategic level (Section 4.3.2.) based on the selected business imperatives. 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.

In order to implement the actual control techniques relevant to those key control areas summarised in Table 1, a business will identify their specific business imperatives. Thereafter, implement the relevant controls that are included in each control area. The detail of these controls can be found in the applicable individual control frameworks.

**Table 1: Key Control Areas That Are Addressed In Combining And Aligning The COBIT, ITIL And ISO 27002 Control Framework's Control Objectives To The Applicable Business Imperatives**

	Business Imperatives												
	Innovation	Affordability	Diverse Products/Lines	Ease Of Use	Regulatory Compliance	Mobility	Reliability	Pro-active Management	Collaboration	Productivity	Customer Service	Replication	
Control Areas Addressed	1.Determine business policies and strategies	X	X	X	X	X	X	X	X	X	X	X	
	2.Implement business-IT alignment procedures	X	X	X	X	X	X	X	X	X	X	X	
	3.Service level management	X	X	X	X	X	X	X	X	X	X	X	
	4.Implement IT resource management	X	X	X	X	X	X	X	X	X	X	X	
	5.Purchase management	X	X	X	X		X	X		X	X	X	
	6.Access controls/ Security management	X	X	X	X	X	X	X	X	X	X	X	
	7.Information system's acquisition, development & maintenance	X	X	X	X	X	X	X	X	X	X	X	
	8.Project management	X		X								X	
	9.Information management	X	X	X	X	X	X	X	X	X	X	X	
	10.Financial management	X	X	X					X		X	X	
	11.Risk management	X	X	X		X	X	X	X	X	X	X	
	12.Change, release and deployment management	X	X	X	X	X	X	X	X		X	X	
	13.Human resource security	X	X	X	X	X	X	X	X	X	X	X	
	14.Problem management	X	X	X	X	X	X	X	X	X	X	X	
	15.Business continuity management					X	X	X	X	X	X	X	
	16.Compliance requirements	X				X	X	X	X			X	
	17.Configuration management	X		X	X	X	X	X	X			X	

A business deciding to address specific business imperatives would need to implement the controls around the affected areas as highlighted by an "X". These business imperatives will form the foundation of implementing IT governance principles. In this manner, IT controls will address all relevant risk areas at a strategic level. The next step will be to implement IT governance principles at an operational level.

#### 4.4 Identify Access Paths And Implement Configuration Controls

The concept of using business imperatives as a foundation for implementing IT controls at a strategic level is continued at an operational level. Each business imperative is affected by different access paths. Since an access path refers to the manner in which an IT user gains access to an IT system, all such possible access paths, relating to

a specific business imperative, should be identified as well as its individual components. These components should be assessed for risks in terms of how it relates to the specific business imperatives defined by a business.

Different access paths will apply for different users based on each user's access rights, restrictions, user profile, and terminal identification settings (Boshoff, 1990). Controlling the relevant access paths' security levels will be dealt with at both an organisational and technological level (Boshoff, 1990). The organisational level includes matters such as segregation of duties and creating valid user profile set-up controls. By implementing the corresponding access path controls and linking them to the relevant user profiles and set-up, the technology level is risk managed.

Each access path's individual IT architectural components (being, *inter alia*, specific hardware, software, network, and other applicable parts) should be identified to determine whether they are correctly *built*, *set up*, *configured*, *maintained*, and/or *operated* (known as configuration controls) (Boshoff, 2010). This is important in order to ensure the risk areas relating to the specific component have been correctly addressed.

The configuration controls are defined as follows:

- Computer hardware is '*built*' by assembling the various components, enabling them to accept an operating system and to function in a computer. Computer software is '*built*' when source code files are created and converted into stand-alone executable software artefacts.
- '*Set-up*' or '*installation*' of a program (including drivers, plug-ins, etc.) refer to implementing the program on a computer system and ensuring the execution thereof.
- The term '*configuration*' refers to the configuration of files or configuring the initial settings of some computer programs. User applications, server processes, and operating system settings are normally configured items.
- A computer is '*operated*' by overseeing the smooth running of a computer/device and intervening in the process by stopping and restarting services or the whole computer.
- '*Maintenance*' ensures that software is upgraded and/or computers/devices are repaired so as to ensure the optimum performance and reliability of such devices.

By implementing the control techniques, as well as the appropriate configuration controls, the risk assessment process is complete and the appropriate risks are addressed at an operational level.

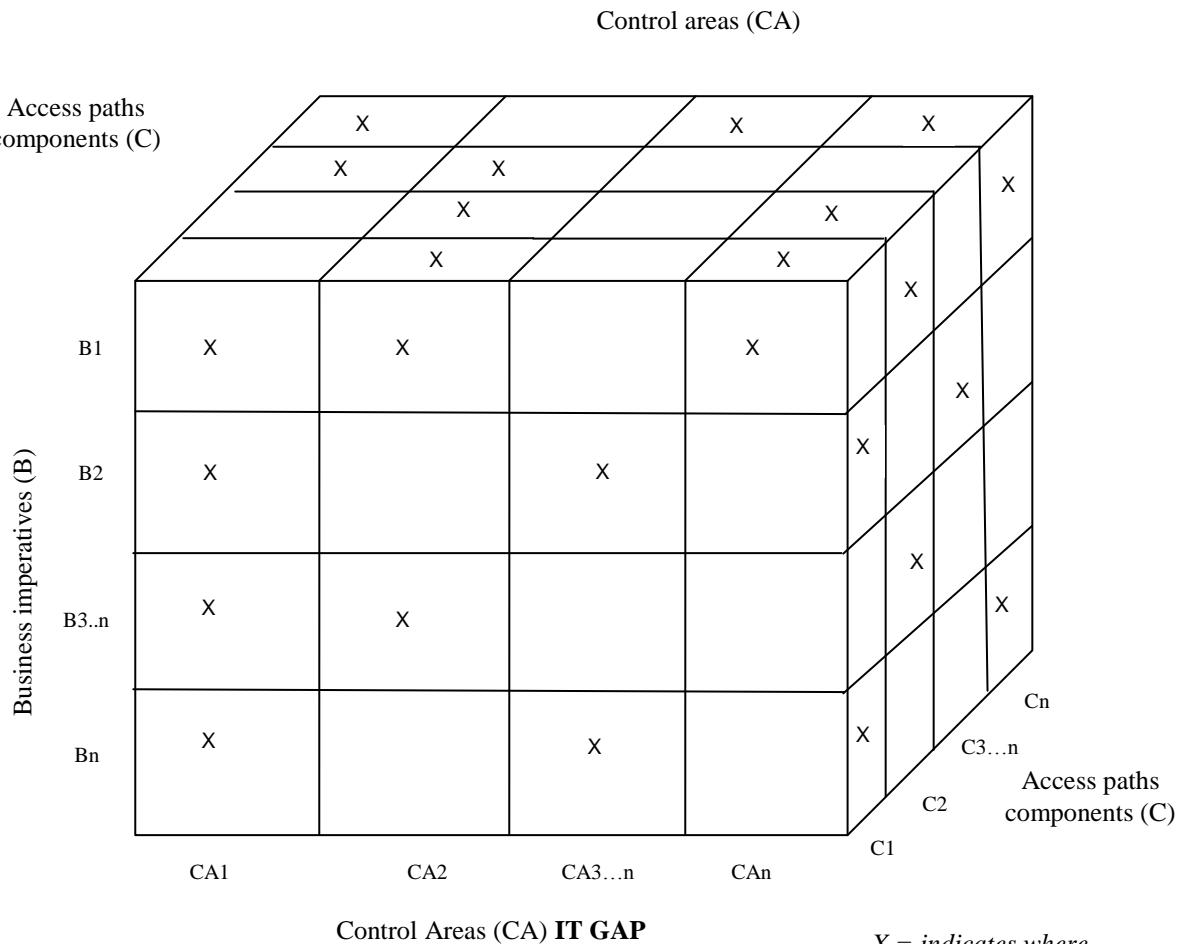
#### **4.5 Theoretical Representation Of The Integrated Framework**

Figure 3 shows a theoretical representation of the interaction between the three main parts of the integrated framework developed in this paper.

The integrated framework can be implemented practically in order to bridge the IT gap in the following manner:

- Identify the appropriate business imperatives applicable to the business and the corresponding control areas (as shown in Table 1) that should be implemented in order to address the risks relevant to the applicable business imperative.
- Identify the relevant access paths and its components. The importance of each component can be evaluated against the applicable business imperative. This step will assist business managers in understanding which controls to implement from an IT point of view, thus bridging the 'IT gap' disparity.
- For each of relevant access path components (as identified in step 2), the relevant control areas, which need to be implemented to address the risks, need to be considered. This step will assist IT management in implementing the relevant controls to ensure a proper control environment has been set up and the appropriate control objective met. Similarly, it will assist IT management in understanding the business factors driving IT.

Figure 3: Theoretical Representation Of The Integrated Framework



## Control Areas (CA) IT GAP

*X = indicates where applicable areas intercept, if applicable*

## 5. CONCLUSION

In recent times, greater emphasis has been placed on governance and, in particular, IT governance. Directors and management have been tasked with the responsibility of implementing IT governance principles. However, most management do not understand the concepts surrounding IT governance and, consequently, implement these principles in an *ad hoc* manner, resulting in an ineffective IT governance system.

The purpose of this study is to provide a practical framework that can be used to effectively implement IT governance principles at a strategic and operational level, using an integrated framework that links the controls in these levels. At a strategic level, rather than using multiple frameworks of a generic nature, a business should identify those specific business imperatives which are applicable to its business, linking them with controls at an operational level in a manner that makes it understandable to both business and IT managers. One of two methods can thereafter be followed by senior management in order to effectively and efficiently address IT governance principles:

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

2. The tool developed in this study (in Table 1), which combines three generally-accepted and used control frameworks into an integrated framework that is linked to a list of generic business imperatives, can be tailored by senior management 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.

Using business imperatives as the foundation, implementing of IT governance principles is continued at an operational level where the relevant control techniques of the applicable key control areas, as identified in steps 1 and 2, can be implemented.

In order to understand the technology underlying the computer system, management should also identify the IT system's access paths and break it up into its components. These components can be analysed by evaluating them against the appropriate business imperatives and control areas of the business.

In this manner, the appropriate level of IT controls is implemented, addressing all the relevant risk areas at a strategic and operational level as well as ensuring addressing IT governance principles. More importantly, it allows management to align IT governance principles at strategic and operational levels. This study provides a basis from which guidance and direction can be taken in order to implement effective IT governance principles.

#### AUTHOR INFORMATION

**Ms. Riana Goosen** is currently a lecturer in management accounting, with previous experience lecturing auditing, as well as accounting, at the Stellenbosch University, South Africa. She qualified as a chartered accountant after graduating with BComm Accounting Honours from the Nelson Mandela Metropolitan University based in Port Elizabeth. After spending a few years working as an external auditor, she pursued a career as a lecturer at the Stellenbosch University where she obtained her Masters in computer auditing. Her interests lie in the King 3 report as well as international corporate governance matters. E-mail: [Goosen@sun.ac.za](mailto:Goosen@sun.ac.za) (Corresponding author)

**Mr Riaan J Rudman** is a Senior Lecturer in Auditing at Stellenbosch University, South Africa. He obtained his Bachelors of Business Science (Finance Honours) degree as well as a Post-graduate Diploma in Accounting from the University of Cape Town. He also holds two masters' degrees: a Masters of Business Science, in the field of finance and a Masters of Accountancy, awarded *cum laude*, in the specialist field of computer auditing. He is a qualified chartered accountant specialising in Financial Institutions. His areas of interest lie in business management and acceptable corporate behaviour in an electronic environment. E-mail: [RJRudman@sun.ac.za](mailto:RJRudman@sun.ac.za)

#### REFERENCES

1. Bakari, J.K., Tarimo, C.N., Yngström, I., 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.
2. 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.
3. Boshoff, W.H. (1990). A path context model for computer security phenomena in potentially non-secure environments. Johannesburg: Rand Afrikaans University. (Unpublished doctoral dissertation).
4. Boshoff, W.H. (2010). Masters in Accounting (Computer Auditing). Stellenbosch: University of Stellenbosch. (Unpublished lecture slides).
5. 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.
6. Carlson, T. (2008). Understanding ISO 27002. Retrieved from:  
[http://www.orangeparachute.com/documents/Understanding\\_ISO\\_27002.pdf](http://www.orangeparachute.com/documents/Understanding_ISO_27002.pdf)
7. Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I., Windebank, J. & Rance, S. (2007). An introductory overview of ITIL V3. Retrieved from: [http://www.best-management-practice.com/gempdf/itsmf\\_an\\_introductory\\_overview\\_of\\_itil\\_v3.pdf](http://www.best-management-practice.com/gempdf/itsmf_an_introductory_overview_of_itil_v3.pdf)

8. Chen, H., Kazman, R. & Garg, A. (2004). BITAM: An engineering-principled method for managing misalignments between business and IT architectures. *Science of Computer Programming*, 57:5-26.
9. Cherry Tree & Company. (2000). Extended Enterprise applications. Retrieved from: [http://www.sysedv.tu-berlin.de/intranet/kc-kb.nsf/bc64cc33c3daf5fec1256979005bc026/F16DB8D8AA21A63DC1256CD300398C69/\\$File/Extended+Enterprise+Applications.pdf?OpenElement](http://www.sysedv.tu-berlin.de/intranet/kc-kb.nsf/bc64cc33c3daf5fec1256979005bc026/F16DB8D8AA21A63DC1256CD300398C69/$File/Extended+Enterprise+Applications.pdf?OpenElement)
10. Drury, C. (2004). *Management and Cost Accounting* (6<sup>th</sup> ed.). London: Thomson Learning.
11. Hardy, G. (2006a). Guidance on aligning COBIT, ITIL and ISO 17799. Retrieved from: <http://www.isaca.org/Journal/Past-Issues/2006/Volume-1/Documents/jpdf0601-Guidance-on-Aligning.pdf>
12. 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.
13. Hill, P. & Turbitt, K. (2006). Combine ITIL and COBIT to meet business challenges. Retrieved from: [http://www.vpit.ualberta.ca/frameworks/pdf/itil\\_cobit.pdf](http://www.vpit.ualberta.ca/frameworks/pdf/itil_cobit.pdf).
14. IBM. (2006). Igniting innovation through business and IT fusion. Retrieved from : [http://www-935.ibm.com/services/fr/cio/flexible/flex\\_wp\\_gts\\_fusion\\_business\\_it.pdf](http://www-935.ibm.com/services/fr/cio/flexible/flex_wp_gts_fusion_business_it.pdf)
15. Innotas. (2010). The CXO's guide to IT governance. A roadmap to driving top-down alignment between business & IT strategy. Retrieved from: [http://solutioncenters.cio.com/innotas\\_governance/registration/5962.html?source=ciozne](http://solutioncenters.cio.com/innotas_governance/registration/5962.html?source=ciozne)
16. Institute of Directors Southern Africa (IODSA). (2009). King Report on corporate governance for South Africa (King III). Retrieved from: [http://c.ymcdn.com/sites/www.iodsa.co.za/resource/resmgr/king\\_iii/king\\_code\\_of\\_governance\\_for\\_.pdf](http://c.ymcdn.com/sites/www.iodsa.co.za/resource/resmgr/king_iii/king_code_of_governance_for_.pdf)
17. ISACA. (2012). 2012 Governance of Enterprise IT (GEIT) survey. Retrieved from: <http://www.isaca.org/Pages/2012-Governance-of-Enterprise-IT-GEIT-Survey.aspx>
18. IT Governance Institute. (2006). COBIT mapping: Overview of international IT guidance, 2<sup>nd</sup> edition. Retrieved from: <http://www.sox-expert.com/uploads/files/COBIT%20Mapping%202nd%20Edition.pdf> .
19. IT Governance Institute. (2007). COBIT 4.1. Online: <http://www.isaca.org/Knowledge-Center/ResearchDeliverables/Pages/COBIT-4-1.aspx>
20. IT Governance Institute. (2008a). Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for business benefit. Retrieved from: <http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT,ITILV3,ISO27002-Bus-Benefit-12Nov08-Research.pdf>
21. IT Governance Institute. (2008b). COBIT Mapping. Mapping of ITIL v3 with COBIT 4.1. Retrieved from: <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-Mapping-Mapping-of-ITIL-V3-With-COBIT-4-11.aspx>
22. IT Governance Institute. (2008c). Understanding how business goals drive IT goals. Retrieved from: <http://www.isaca.org/Knowledge-Center/Research/Documents/Understand-Bus-Drive-IT-Goals-15Oct08-Research.pdf>
23. Johnston Turner, M., Oltzik, J. & McKnight, J. (2009). Security management survey: ISO, ITIL and COBIT triple play fosters optimal security management execution. Retrieved from: [http://www.bsmreview.com/security\\_best\\_practice\\_survey.shtml](http://www.bsmreview.com/security_best_practice_survey.shtml)
24. Kosutic, D. (2010). ISO 27001 vs ISO 27002. Retrieved from: <https://www.infosecisland.com/blogview/8055-ISO-27001-vs-ISO-27002.html>
25. Liell-Cock, S., Graham, J. & Hill, P. (2009). IT governance aligned to King III. Retrieved from: <http://lgict.org.za/sites/lgict.org.za/files/documents/2009/liell-cock-graham-hill-2009-it-governance-aligned-king-iii.pdf>
26. Maxi-Pedia Encyclopedia. (2011). ISO 27001. Retrieved from: <http://www.maxi-pedia.com/ISO+27001>
27. Muller, R. (2009). IT governance report slated. Retrieved from: <http://mybroadband.co.za/news/general/7242-it-governance-report-slated.html>
28. Numara Software. (2009). Show me the money. How life in the ITIL fast lane can deliver success. Online: <http://www.findwhitepapers.com/whitepaper7394>
29. Olivier, S. (2012). Good corporate governance in South Africa. Retrieved from: [http://www.communicate.co.za/\\_blog/Communicate\\_Blog/post/Good\\_Corporate\\_Governance\\_in\\_South\\_Africa/](http://www.communicate.co.za/_blog/Communicate_Blog/post/Good_Corporate_Governance_in_South_Africa/)
30. Rudman, R.J. (2011). IT governance failure. *Auditing SA*, Summer 2010/2011:37 – 39.

31. Rudman, R. J. (2010). Framework to identify and manage risks in web 2.0 applications. *African journal of business management*, 4(13): 3251 – 3264.
32. Rudman, R.J. (2008a). Demystifying COBIT. Retrieved from:  
<http://www.accountancysa.org.za/resources>ShowItemArticle.asp?ArticleId=1398&Issue=979>
33. Rudman, R.J. (2008b). IT governance: a new era. *Accountancy SA*, March 2008: 12 – 14.
34. Sahibudin, S., Sharifi, M. & Masarat, A. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. *Second Asia International Conference on Modelling & Simulation*, 2008. Retrieved from:  
<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4530569>
35. Santarcangelo, M. (2010). Configuration auditing – the next critical step in compliance. Retrieved from:  
<http://www.ncircle.com/pdf/papers/nCircle-WP-ConfigurationAuditingNextStep-1064-03.pdf>
36. Simkova, E. & Basl, J. (2006). Business value of IT. Retrieved from:  
<http://si.vse.cz/archive/proceedings/2006/business-value-of-it.pdf>
37. Smit, S. (2009). Defining and reducing the IT gap by means of comprehensive alignment. Stellenbosch: University of Stellenbosch. (Unpublished master's thesis).
38. 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.
39. The Economist. (2006). Great expectations: The changing role of IT in the business. September 2006. Retrieved from: [http://graphics.eiu.com/ebf/PDFs/GTF\\_article\\_1\\_September\\_06\\_FINAL.pdf](http://graphics.eiu.com/ebf/PDFs/GTF_article_1_September_06_FINAL.pdf)
40. Tripwire Incorporated. (2007). Winning the IT Control game: using configuration audit and control to improve efficiency and control risk. Retrieved from:  
[http://www.aservo.com/fileadmin/user\\_upload/downloads/tripwire/Tripwire\\_Winning\\_the\\_IT\\_Control\\_Game\\_WP.pdf](http://www.aservo.com/fileadmin/user_upload/downloads/tripwire/Tripwire_Winning_the_IT_Control_Game_WP.pdf)
41. Voogt, T. (2010). IT governance, Dear CFO, what should you do? Retrieved from:  
<http://www.accountancysa.org.za/resources>ShowItemArticle.asp?ArticleId=2044&Issue=1097>
42. Wallhoff, J. (2004). Combining ITIL with COBIT and ISO/IEC 17799:2000. Retrieved from:  
<http://www.scillani.se/assets/pdf/Scillani%20Article%20Combining%20ITIL%20with%20Cobit%20and%2017799.pdf>

**NOTES**