# THE DEVELOPMENT OF AN INTEGRATED FRAMEWORK IN ORDER TO IMPLEMENT INFORMATION TECHNOLOGY GOVERNANCE PRINCIPLES AT A STRATEGIC AND OPERATIONAL LEVEL FOR MEDIUM-TO-LARGE SIZED SOUTH AFRICAN BUSINESSES

by
Riana Goosen

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

Supervisor: Mr. Riaan J. Rudman
Faculty of Economic and Management Sciences

March 2012

Declaration

By submitting this thesis/dissertation electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

March 2012

## ACKNOWLEDGEMENTS

I am truly thankful and appreciative to everyone who has contributed and made this research project possible. I would like to thank the following people in particular,

- To the one and only living God and Jesus Christ I worship, thank you God for giving me the talents and abilities to be able to do this project.

- To my parents, who have always believed in me, thank you for giving me wings to fly on and make all my dreams come true.

- To Riaan Rudman, thank you for your patience, guidance and input. I could not have asked for a better mentor.

## ABSTRACT

In today's technologically advanced business environments, Information Technology (IT) has become the centre of most, if not all businesses' strategic and operational activities. It is for this reason that the King III report has dedicated a chapter to IT governance principles, in effect making the board of directors and senior management responsible for implementing such principles. King III's guidance on these principles is only described in broad terms and lack sufficient detail as how to implement these principles. Though various guidelines, in the form of IT control frameworks, -models and -standards exist, it remains highly theoretical in nature and companies tend to view these control frameworks, -models and -standards on an individual basis, implementing them in an ad hoc manner, resulting in the implementation of an inefficient IT governance system, that does not address the key strategic areas and risks in a business.

The purpose of this study is to develop an IT best practices integrated framework which 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 a best practice control framework, -model and -standard, including its underlying processes.

By combining and aligning the relevant processes of the control framework, -model and -standard to the business' imperatives, a framework was developed to implement IT governance principles at a strategic level. The integrated framework is extended to provide guidance on how to implement good IT controls at an operational level. The control techniques, of the applicable processes identified at a strategic level, are implemented as well as the controls around a company's various access paths, which are affected by a company's business imperatives. These access paths are controlled through the implementation of applicable configuration controls. By making use of the integrated framework which was developed, an effective and efficient IT governance system can be implemented, addressing all applicable IT risks relevant to the key focus areas of a business.

**UITTREKSEL**

In vandag se tegnologies gevorderde besigheids omgewings het Informasie Tegnologie (IT) die middelpunt geraak van die meeste, indien nie elke onderneming se strategiese en operasionele aktiwiteite nie. Dit is vir hierdie rede dat die King III verslag ‘n hoofstuk aan die beginsels van IT korporatiewe beheer wy. Dié verslag hou die direkteure en bestuur verantwoordelik vir die implementering van hierdie beginsels. Die King III verslag verskaf egter slegs in breë trekke leiding in verband met die implementering van hierdie beginsels en ‘n gebrek aan meer gedetailleerde beskrywings bestaan. Alhoewel verskeie riglyne, in die vorm van IT kontrole raamwerke, -modelle en -standaarde bestaan, bly dit steeds teoreties van aard en is maatskappye geneig om hierdie riglyne op ‘n individuele vlak te hanteer en op ‘n willekeurige wyse te implementeer. Hierdie proses lei tot die implementering van ‘n ondoeltreffende IT korporatiewe beheerstelsel.

Die doel van hierdie studie is om ‘n geïntegreerde beste praktykraamwerk te ontwikkel wat deur die direkteure en bestuur van ‘n onderneming gebruik kan word om op beide ‘n strategiese en operasionele vlak ‘n doeltreffende IT korporatiewe beheermaatstelsel in plek te stel. ‘n Geïntegreerde raamwerk is ontwikkel deur ‘n volledige literatuurstudie uit te voer, gebaseer op ‘n beste praktyk IT kontrole raamwerk, -model en -standaard en die gepaardgaande prosesse.

Deur die toepaslike prosesse van hierdie kontrole raamwerk, -model en -standaard te kombineer en te belyn met ‘n besigheid se besigheidsimperatiewe, word IT korporatiewe beheerbeginsels op ‘n strategiese vlak in plek gestel. Die geïntegreerde raamwerk sluit riglyne in om goeie IT kontroles op ‘n operasionele vlak te implementeer. Die kontrole tegnieke, wat verbind word met die gepaardgaande prosesse wat tydens die strategiese vlak geïdentifiseerd is, word geimplementeer asook die die toepaslike konfigurasie kontroles oor die verskeie toegangspaaie wat beïnvloed word deur ‘n besigheids se besigheidsimperatiewe. Deur gebruik te maak van die ontwikkelde geïntegreerde raamwerk kan alle geaffekteerde IT risikos nou aangespreek word en ‘n doeltreffende IT korporatiewe beheerstelsel in plek gestel word.

# TABLE OF CONTENTS

# LIST OF FIGURES, TABLES AND APPENDICES

## Figures



## Tables



## Appendices

# CHAPTER 1: INTRODUCTION

## 1.1 Background

Good corporate governance principles are important aspects to consider for 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. The first two King reports addressed the importance of corporate governance, risk management and sustainability matters. The third King report highlights the implementation of strong information technology (IT) governance principles. It states that the board of directors and senior management are held responsible for implementing these IT governance principles (Institute of Directors Southern Africa (IODSA), 2009).

The rationale for including IT governance matters in the latest 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 global 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. As a consequence, companies can no longer afford for their IT division to be held solely responsible for IT-related matters.

This poses a challenge as King III's guidance to senior management and directors, specifically with regard to how to practically implement these IT governance requirements, seems vague and unclear (Muller, 2009) and only addresses these areas at a high-level. A number of best practice IT control frameworks, -models and -standards are available to be used to develop and implement a high quality IT governance system. Business- and IT management are required to work together in the implementation of this system. However, an 'IT gap' has evolved between these two parties' different understandings of the required control frameworks, -models and -standards. The two parties also differ in terms of how to implement and align these IT principles to a company's business objectives, in order to create an environment in which business and IT objectives are aligned (Rudman, 2011).

This gap is further widened by the amount of time and money which is spent on completing IT governance compliance questionnaires (Rudman, 2011), which attempt to implement IT controls, without effectively addressing the business' IT risk areas. This results in the implementation of an inefficient IT governance system (Rudman, 2010). In order to overcome this gap and the ad hoc implementation of controls, a company should not assume that all business areas carry the same IT risk profile, but should recognise different risk profiles for each area and implement the appropriate IT controls, based on a specific foundation.

The purpose of this study is to develop an integrated framework, which will provide guidance in how to effectively and efficiently implement IT governance principles at a strategic and operational level, through performing the appropriate risk assessment procedures and implementing the appropriate controls at these two respective levels.

### 1.2 Historical review

Research on the implementation of an effective IT governance system, by implementing best practice IT control frameworks, -models and -standards, and achieving business-IT alignment in a business has been documented in various forms, which each discuss different areas of this all encompassing topic.

In 2006 the Information Technology Governance Institute (ITGI) performed a high level mapping between The Control Objectives for Information and related Technology (version four) (COBIT) framework's control processes and objectives and the following individual control guidelines, -frameworks, -models and -standards:

- The Committee of Sponsoring Organisations of the Treadway Commission (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).

The ITGI further performed a mapping between the processes of the IT best practice control framework COBIT, the control model ITIL and the ISO 27002 standard in order to implement and combine these control framework, -model and –standard's best processes in order to effectively implement a strong IT control environment (ITGI, 2008a). The ITGI also produced a document discussing how IT goals are driven by business goals, and how to align these IT goals with business goals (ITGI, 2008c).

Smit (2009) attempted to define the 'IT gap' concept, which exists in this business-IT alignment process. Generic business imperatives were identified and these business imperatives were aligned to the COBIT control framework's processes, in order to reduce the 'IT gap'. Steenkamp (2011) and Hardy (2006b) showed that, by implementing COBIT processes, 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 addresses the implementation of IT governance principles and the achievement of aligning business and IT objectives at a strategic level. IT governance principles should also be addressed at an operational level, as noted by Boshoff (1990), who formulated the concept of an 'access path' and discussed its significance in the IT environment. This idea was further extended in Santarcangelo's (2010) discussion on the importance of controlling the risks surrounding these access paths with the implementation of appropriate configuration controls.

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 certain aspects of the IT governance alignment process in isolation and do not address these aspects at a combined and integrated level.

## 1.3 Research problem and objective

The study proposes to address the lack of guidance relating to the implementation of IT governance provided in the King III report, and to provide a solution to the IT gap problems.

The objective of this study is to develop an integrated framework which can assist senior management and directors in practically implementing King III's IT governance principles at both a strategic and operational level, and in addressing the appropriate risk areas by implementing the relevant control processes of a best practice IT control framework, -model and -standard as well as the configuration controls and control techniques at the respective strategic and operational levels.

## 1.4 Scope of the research

The research study is subject to the following constraints:

Each company's business imperatives are different at a strategic level. It is not the purpose of this study to provide industry-specific business imperatives, but rather to provide broad-based imperatives, which could be adapted to most industries and companies. Any additional company-specific imperatives should be identified and implemented by management, according to each company's unique business environment. The research was also limited to business imperatives which could impact on IT-related matters, and are thus relevant to the IT governance principles.

The concepts surrounding access paths and the implementation of their corresponding configuration controls will only be discussed at a high level, due to these concepts being highly detailed in nature.

The implementation of the integrated framework developed in the study is most appropriate in medium and large sized companies, since the implementation of such an integrated framework can become a time consuming and expensive task, in which the implementation costs, could exceed the benefits available to a smaller company.

## 1.5 Research motivation

Most advice provided to board members and senior management relates to structural, composition, financial and independence matters. Guidance on IT governance matters and IT risk management is not readily available (Hardy, 2006b).
As described in section 1.2, most research discusses the application of individual control frameworks, -models and -standards in a business environment, concentrating more on the theoretical aspects of implementation than on providing practical guidance on how to integrate such control frameworks, -models and -standards. A practical integrated framework is required to allow senior management to focus on and address the key IT risk areas. This will ensure that an effective and efficient IT governance system is put in place.

## 1.6 Organisation of the research

The thesis will consist of the following chapters:

- **Chapter 2: Research methodology:** A detailed literature review was performed and an integrated framework was subsequently developed, based on the findings from the literature review.
- **Chapter 3: Literature review:** A literature review 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.
- **Chapter 4: Findings on implementing IT governance principles at a strategic and operational level:** A best practice integrated framework was developed from this alignment process in order to implement IT governance principles at a strategic and operational level. The findings include the identification of broad-based business imperatives, and the alignment between these business imperatives and the processes of a best practice control framework, -model and -standard.
- **Chapter 5: Conclusion:** This chapter contains 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 and operational level.

# CHAPTER 2: RESEARCH METHODOLOGY

## 2.1 Purpose of the study

The aim of this study is to develop an integrated framework, to implement IT governance principles at a strategic and operational level. The study is non-empirical in nature and is based on an extensive literature review. An integrated framework was developed by following a deductive strategy, based on the findings of the literature review.

## 2.2 Literature study

The literature review covered guidelines by local and international governance institutions, papers published in accredited research journals, articles in popular publications and websites, as well as relevant domestic master's and doctoral theses and dissertations, covering the following areas:

- The importance of corporate governance, specifically focusing on IT governance principles, including the King III report and international related IT governance concepts,
- Senior management's key roles and perceptions surrounding the implementation of IT governance principles,
- The 'IT gap' problem and business-IT alignment processes,
- The basic business assumptions and the business imperative concepts,
- A best practice IT control framework, -model and -standard, and
- Access paths and configuration control concepts.

## 2.3 Research methodology

IT governance principles are implemented at a strategic level by identifying a company's strategic business imperatives and mapping the processes of a best practice IT control framework, -model and -standard to these business imperatives.

Despite the fact that basic IT controls exist at the basic business assumption level, companies often neglect to address the risks they are exposed to with regard to their business imperatives. It is at this level that the risk of non-alignment between IT and

company objectives lies. Business imperatives, and not basic business assumptions, drive the vision and direction of any company. These business imperatives were therefore selected to form the foundation of the integrated framework which aims to implement good IT governance principles in a company (Boshoff, 2010) as well as achieve business-IT alignment. In order to develop this integrated framework, the following steps were followed:

***Step 1:*** A broad-based set of business imperatives was identified.

***Step 2:*** The most relevant best practice IT control framework, -model and -standard suitable for inclusion in the development of the integrated framework model were identified. Since different IT best practice control frameworks, -models and -standards exist, the guidance outlined below, provided by Liell-Cock *et al* (2009), was followed in deciding which best practice control frameworks, -models and -standards should be selected.

***i) Factors considered in deciding which control frameworks, -models and -standards should be implemented:***

- *The control framework, -model and -standard has a business-orientated focus, ensuring business objectives are aligned with the IT activities and objectives.*
- *It provides core guidelines in establishing a set of internal controls so as to prevent, detect and correct undesirable events.*
- *It addresses most or all IT areas and activities and presents a logical and manageable structure of such IT activities.*
- *It is generally accepted as being a best practice control framework, -model and -standard.*
- *It supports risk management and provides the necessary controls to uncover IT issues.*
- *It supports the company in adhering to relevant laws and regulations.*
- *It contains performance measures so as to ascertain whether the implementation thereof succeeded or failed.*

Several control frameworks, -models and -standards were evaluated against the above-mentioned criteria and it was found that the best control framework, -model and -standard to implement for the purpose of this study, were the COBIT control framework, the ITIL control model and ISO 27002 (supported by ISO 27001) standards, since this control framework, -model and -standard are internationally

recognised and adaptable to most industries. COBIT provides guidance for the implementation of IT governance related controls and perform a high level risk assessment on the general control environment. ITIL identify 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). Due to the fact that this selected IT best practice control framework, -model and -standard contain a great amount of detail, the focus of this study was limited to identifying internal controls in keeping with the COSO's definition of an internal control.

***ii) Definition of internal control***

*COSO (ITGI, 2006) defines an internal control as being a process, affected by an entity's board of directors, management and other personnel. It is designed to provide reasonable assurance regarding the achievement of objectives in the following categories:*

- *Effectiveness and efficiency of operations,*
- *Reliability of financial reporting, and*
- *Compliance with applicable laws and regulations.*

*COSO provides five components which form part of the internal control concept:*

- ***Control environment:*** *The control and risk conscious environment in which people operate is set by senior management and directors, and will influence people's behaviour, ethical values and competencies.*
- ***Risk assessment:*** *Establish a risk management policy, so as to identify, analyse and manage risks appropriately.*
- ***Control activities:*** *Implement sound policies and procedures, so as to manage risk areas and achieve a company's business objectives.*
- ***Information and communication:*** *An information and communication system must be implemented, to ensure that people can carry out their responsibilities, including control activities.*
- ***Monitoring:*** *Monitor the internal control framework, -model and -standard on a continuous basis and make corrections and adjustments, where deemed necessary.*

The controls selected in Appendices 1-3 will therefore include some or all of these elements described above.

***Step 3.1:*** A detailed study of the COBIT control framework was performed, identifying the relevant COBIT processes which are applicable to the specific business imperatives.
***Step 3.2:*** The relevant COBIT processes were aligned to business imperatives as shown in Appendix 4.

***Step 4:*** The processes of the ITIL control model and ISO 27002 standard were mapped to the relevant COBIT control framework's processes, which are relevant to the business imperatives identified in step 2 above. Appendix 5 contains a high level summary of this mapping. The detail of the individual control techniques mentioned in Appendix 5, can be found in the relevant Appendices 1, 2 or 3. (The detail provided in Appendices 1,2,3 and 5 will be used at an operational level, but were also necessary for the procedures mentioned in step 5, which is to be used at a strategic level.)

***Step 5:*** The mapping performed between the business imperatives and the COBIT processes, as mentioned in step 3, was subsequently combined with the mapping of the processes of the control framework, -model and -standards performed in step 4. In aligning the processes of the control framework, -model and -standard to the business imperatives, it was noted that certain key control areas were covered repetitively. A summary was made of these key control areas that must be addressed, at a strategic level, when a specific business imperative is chosen. A high level summary of these key control areas is documented in section 4.4.1.

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

***Step 6:*** The control techniques mentioned in Appendix 1, 2, 3 and 5 (as mentioned in step 4 above) were used to implement the appropriate IT controls at an operational level.

***Step 7.1:*** The definition of access paths were described at a conceptual level. The different components of each access path were also discussed.

***Step 7.2:*** A high level discussion was conducted on the management of the risks surrounding access path components by means of the implementation of configuration controls.

In order to add depth to the findings, the following exercise was performed to confirm that IT governance principles are in fact achieved at a strategic and operational level:

***Step 8.1:*** A mapping exercise was performed between the COBIT processes, the key international IT governance areas and King III's IT governance principles, as shown in Appendix 6.

***Step 8.2:*** As per Appendix 4, the business imperative's relevant COBIT processes were mapped to Appendix 6's results, achieving an alignment between business imperatives, its relevant COBIT processes, key international IT governance areas and King III's IT governance principles, as shown in Appendix 7.

The result of this final mapping confirms that, by using business imperatives as a starting point, one is able to comply with all of King III's IT governance requirements at both a strategic and operational level.

## 2.4 Conclusion

By implementing the above-mentioned methodology at both a strategic and an operational level, it will be shown that compliance with IT governance principles is possible at both the strategic and operational levels.

# CHAPTER 3: LITERATURE REVIEW

## 3.1 Introduction

IT governance consists of a number of individual elements, which need to be viewed on an integrated level. These elements, such as governance-related matters, the 'IT gap' problem, business imperatives, as well as the definition of access paths, for example, were further investigated so as to obtain a better understanding of their functional roles in achieving IT governance principles. Certain best practice IT control framework, -model and –standards were also researched in detail. When these elements are combined, the integrated framework can be practically implemented, thereby achieving IT governance requirements and addressing all relevant risks at both a strategic and operational level.

## 3.2 King III report and governance

### 3.2.1 Corporate governance

Corporate governance can be viewed as the overall business structure and ethical values which determine a company's direction and performance standards. It involves the board of directors, senior management, shareholders, employees and any other related parties. It also aims to align the interest of individuals with the goals of the company and society (McRitchie, 1999).

Good corporate governance policies ensure that appropriate controls are in place, creating a strong control environment which ensures that ethical, responsible, accountable, fair, transparent and reliable actions are performed by all parties (IODSA, 2009). IT governance is seen as an integral part of the overall corporate governance framework and should be managed in the same effective and efficient manner.

### 3.2.2 IT governance

According to the King III report, 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 company's specific requirements, so as to ensure that a company achieves its strategic objectives (IODSA, 2009). The IT governance framework includes the human, financial, physical and informational aspects of IT (Doughty & Grieco, 2005).

In today's advanced technology environments, IT has become the centre of any business activity and has an impact on both operational and strategic levels. IT should be able to ensure reliable sources of information (Voogt, 2010), which are free from financial and reputational damages caused by security breaches, errors and hacker attacks (Hardy, 2006b). In addition, IT strategies, policies, budgets and good IT investment returns will only be achieved when good IT governance practices are implemented (Voogt, 2010).

### 3.2.3 The advantages of implementing strong IT governance principles

Bowen, Cheung and Rohde (2007) and Hardy (2006b) discussed the following advantages which 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 by strategically aligning IT with business goals and processes, making business operations more efficient and effective.
- 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 possible and risk management procedures are maximised by implementing good IT controls.

### 3.2.4 The risks of not complying with good IT governance principles

The following risks are present if good IT governance practices are not implemented (IODSA, 2009):

- Operational risk increases.

- There is a loss of confidentiality, integrity and authenticity of information systems.
- Systems become less available, less reliable and function less effectively.
- Unauthorised use, access and changes to IT systems become a greater risk.

### 3.2.5 Directors' roles and responsibilities

The extent to which IT supports business decisions and how involved management is in making important IT decisions will determine how successful a business will be and vice versa (Kordel, 2004). Directors seem 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 regarded as the IT department's responsibility (Raghupathi, 2007). In some instances, the IT department is regarded as a separate functional area and not managed as an integral part of all business areas (Kordel, 2004).

This was confirmed by Voogt (2010), who cited the South African Institute of Chartered Accountants' (SAICA) research in 2010 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. It has therefore become critical for directors and managers to familiarise themselves with their new roles and responsibilities in respect of King III's IT governance principles.

### 3.2.6 Implementing IT governance principles

The King III report (IODSA, 2009) highlights seven key IT governance principles that must be implemented. Table 1 illustrates King III's IT governance principles, aligned

with the international standards of IT governance, confirming the strong correlation that exists between local and international IT governance standards.

**Table 1 – King III's IT governance principles mapped to international IT governance standards**

| Principle number | King III IT governance principle | International IT governance areas covered by King III |
|---|---|---|
| 5.1 | The board should be responsible for information technology governance. | Strategic alignment, value delivery, performance measurement |
| 5.2 | IT should be aligned with the performance and sustainability objectives of the entity. | Strategic alignment, performance measurement |
| 5.3 | The board should delegate the responsibility for the implementation of an IT governance framework to management. | Resource management, risk management |
| 5.4 | The board should monitor and evaluate significant IT investments and expenditure. | Resource management, value delivery, performance measurement |
| 5.5 | IT should form an integral part of the entity's risk management process. | Risk management |
| 5.6 | The board should ensure that information assets are managed effectively. | Strategic alignment, resource management, risk management, performance measurement |
| 5.7 | A risk committee and audit committee should assist the board in carrying out its IT duties. | Risk management, performance measurement |

International IT governance principles, listed in Table 1, have been categorised into the following five areas (Liell-Cock *et al* 2009):

- **Strategic alignment:** Ensure that IT is aligned with the business' corporate objectives.
- **Value delivery:** Deliver value-added IT services to the business through the optimisation of IT expenditure.
- **Risk management:** Identify and manage IT-related risks and their business impact.

- **Resource management:** Manage the people, data and technology aspects.
- **Performance measurement:** Monitor and control IT's performance in order to achieve the business' goals.

In order to practically implement these principles, 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.

### 3.3 'IT gap'

During the implementation of the above-mentioned IT governance principles, miscommunication between the senior management of a company (ultimately responsible for providing 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 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.

The IT gap exists because of the following reasons:

- Business managers do not understand the technological environment in which the company operates, nor the extent to which IT can support the achievement of the business objectives (The Economist, 2006).
- There is a misalignment between IT and business elements due to business and IT environments constantly changing (Chen, Kazman & Garg, 2004).
- The IT department has its own objectives, which differ from the business executives' objectives for IT (Simkova & Basl, 2006).

A business-IT alignment process must be implemented in order to overcome this gap that exists between IT and business managers' perceptions surrounding IT matters.

## 3.4 Business-IT alignment

### 3.4.1 Defining business-IT alignment

In order for a company to successfully achieve a business-IT alignment environment it is important that an enterprise's strategic and business objectives should 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).

### 3.4.2 Advantages of business-IT alignment

The following advantages are present when the business-IT alignment process has been successfully implemented (IBM, 2006; Innotas, 2010):

- IT strategies become aligned with and supportive of the strategic business goals.
- Business and IT-related risks are reduced.
- Enterprise platforms and architectures are consolidated.
- Reliable real-time data improves decision-making processes.
- There is better access to new market segments, satisfying new and existing customers' needs and maximising capital investment possibilities.
- Strategic flexibility is increased and costs are reduced.

However some businesses still do not comprehend the value and importance of the alignment process (Smit, 2009) and where no alignment or misalignment occurs, the following risks can be present.

### 3.4.3 Consequences of misalignment between business' and IT's objectives

The following risks are possible when business-IT alignment is not achieved:

- 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).

- There is 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).
- There is 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 company will need to implement an integrated framework. The starting point of the framework requires a company to distinguish between their basic business assumptions and business imperatives.

### 3.5 Basic business assumptions and business imperatives

In order for a company 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. The differences between these two concepts are explained below:

#### 3.5.1 Basic business assumptions

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 assumptions*. 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 assumptions include:

- A profit-orientated focus,
- Good internal and accounting controls and standards,
- Critical resource management procedures,
- Business continuity policies and procedures, and
- Data accuracy and security matters (Boshoff, 2010).

Adequate basic IT controls are put in place to address the risks occurring at the basic business assumption 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 (Boshoff, 2010).

### 3.5.2 Business imperatives

Business imperatives are those objectives, selected at a strategic level, that are seen as 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). The business-IT alignment process will be achieved by implementing an integrated framework, using a company's business imperatives as the foundation.

## 3.6 Integrated framework

### 3.6.1 The relevance of an integrated framework

An integrated framework is more suited to companies which have the following structures in place:

- There is a need to comply with regulatory requirements.
- The company has developed operational environments that foster cooperation and collaboration across business, IT and security areas.
- An active information security system is in place.
- The company has more advanced technologies implemented in its operational areas (Johnston Turner, Oltsik & McKnight, 2009).

### 3.6.2 Advantages of using multiple and best practice frameworks

By implementing and integrating the IT governance and internal control guidance of the chosen control framework, -model and -standards, the following advantages can be achieved (Hardy, 2006a; ITGI, 2007; ITGI, 2008a; Johnston *et al,* 2009; NUMARA, 2009):

- Internationally accepted standards are adopted, which provide the best industry practices.
- Best practices help to meet regulatory and legal requirements for IT controls in privacy and financial reporting areas.
- This control framework, -model and-standard are highly adaptable to unique business requirements for different types of enterprises.
- A competitive advantage is gained by creating greater trust and credibility with the business' partners, clients, relevant third parties and regulators.
- Internal costs are optimised by following standardised, rather than specially developed, implementation approaches which make less use of experts.
- Considerable savings on operating, security, legal and insurance costs are achieved, resulting in a better return on IT investments.
- There is a strong focus on aligning IT with business goals.
- More effective organisational, operational, workflow and communication structures are created across the diverse IT and security operational groups.
- The use of scarce IT resources is optimised.
- 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.
- IT governance-related activities are performed in an effective and efficient manner.
- Entities can address complex IT-related risks, such as network security issues.
- A generally accepted standard or benchmark is created for performance assessment of a company against its competitors.
- There is greater control over the infrastructure, resulting in systems being more reliable, available and predictable.

### 3.6.3 Disadvantages of implementing best practice frameworks

Best practice control framework, -model and -standard may, however, be rather arduous to implement. In addition, they can be time consuming, paper intensive, require significant resources and can become a cost intensive exercise (Rudman, 2008b).

By combining and aligning the processes of the below-mentioned control framework, -model and –standards, the integrated framework's best practice processes are identified which can be implemented at both a strategic and operational level, in order to address IT governance matters.

### 3.7 COBIT control framework

Reliable controls must be put in place to ensure that a good IT governance structure is implemented. The COBIT control framework describes what type of controls should be implemented.

#### 3.7.1 COBIT defined

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). 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. Each domain summarises the relevant processes involved. Each process is evaluated, the risks are identified and the impact thereof is rated, either as high, medium or low. 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 described below:

- **Plan and Organise:** This domain focuses on defining and establishing the organisational and infrastructural policies that should be implemented in order to optimally utilise IT resources and assist the company in achieving its business objectives (Sahibudin *et al*, 2008).

- **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 in order to prolong the life of an IT system and its components (Sahibudin *et al*, 2008).

- **Deliver and Support:** This area focuses on the service delivery aspects of IT, including the security, support and training issues (Rudman, 2008a).

- **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 processes comply with the internal and external auditors and with the relevant laws and regulations standards (Sahibudin *et al*, 2008; Rudman, 2008a).

A high level summary of these domains and its processes is provided in Appendix 1.

### 3.7.2 When to use COBIT

Smaller versions of COBIT can be implemented in smaller business environments, however COBIT is normally implemented where:

- A sufficiently large IT infrastructure, with standard or automated IT processes exists.
- A need exists for IT governance implementation and a framework to ensure a quality management system.
- A need exists for an alignment between IT and business goals.
- IT governance procedures are required due to regulatory requirements or pressure from external parties, such as auditors.
- The benefits of implementing COBIT will exceed its costs (Rudman, 2008a).

### 3.7.3 Advantages of implementing COBIT

Rudman (2008a) and ITGI (2007) summarised the following advantages, specifically relating to the COBIT framework:

- COBIT is a freely available and open standard, which reduces implementation costs.
- COBIT can easily be aligned with other internationally accepted control frameworks, -models and -standards ensuring all IT aspects are covered.
- COBIT establishes a strong IT process model by providing strong IT control guidelines.

- The majority of IT processes are covered, providing a uniform approach to all IT areas.
- COSO requirements, with regards to the IT control environment, are met.

### 3.7.4 Disadvantages of implementing COBIT

Rudman (2008a) highlighted the following incremental disadvantages which are specifically applicable when the COBIT framework is implemented:

- COBIT does not provide technical guidance regarding how the controls should be implemented, but rather focuses on which controls should be implemented. Other control models, such as ITIL and ISO 27001 and 27002 standards, provide the detail of the implementation process.
- COBIT does not deal with information security issues, since only one of the 34 processes refers to security matters.

### 3.7.5 Consequences of not complying with COBIT

The following risks are present if COBIT is not implemented (ITGI, 2006):

- Misaligned IT services can create a weak support system for the achievement of business goals.
- The company will continue to view IT as a separate, non-integrated functional area.
- A gap between management's measurements and expectations creates dissatisfied IT users.
- Excessive IT costs and overheads are present.
- Erroneous investment decisions are made due to misaligned IT resources.

## 3.8 ITIL control model

In any business, the quality IT services will determine the quality of the collection, analysis, production and distribution of information. Consequently, IT services are seen as crucial and strategic organisational assets in which the appropriate levels of resources should be invested, so as to enable the support, delivery and management of these critical services. However, IT service delivery aspects often go unaddressed

in organisations (Cartlidge, Hanna, Rudd, MacFarlane, Windebank & Rance, 2007). One way to address IT matters is by implementing a good IT service management system, namely the Information Technology Infrastructure Library (ITIL) framework.

### 3.8.1 ITIL defined

ITIL is a control model that describes best practices in the IT service management areas. It provides a model which implements 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 (Cartlidge *et al*, 2007; Hill & Turbitt, 2006). The ITIL framework consists of the following five categories (Cartlidge *et al,* 2007; Sahibudin *et al,* 2008):

- **Service strategy:** This section provides guidance on how to develop and implement service management principles, and how to transform such principles into strategic assets in order to achieve the company's strategic goals.

- **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, thereby ensuring that the application can function in normal, abnormal and extreme circumstances is supported 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 aspects that support the delivery of these services. Strategic objectives are ultimately realised through this area, therefore making this a critical capability.

- **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.

A high level summary of ITIL's key processes and activities is provided in Appendix 2.

### 3.8.2 When to use the ITIL control model

ITIL will be used by companies that are interested in optimising their IT service management systems (IBM, 2009) and who would like to achieve an effective business-IT alignment focus (Cartlidge *et al*, 2007).

### 3.8.3 Advantages of implementing ITIL

The following additional advantages specifically relate to implementing the ITIL control model as discussed by Cartlidge *et al* (2007), IBM (2009) and NUMARA (2009):

- ITIL provides a good starting point in improving service management processes.
- It improves business productivity levels due to the delivery of higher quality IT services, resulting in improved decision making processes, business profits and revenues.
- ITIL reduces incident handling times.
- ITIL improves customer satisfaction and customer relationships.
- It emphasises the importance of creating business value, rather than simply just executing processes.
- ITIL can be applied in today's modern web-centric environments. It is also closely integrated with business processes and is more business-need orientated.

### 3.8.4 Disadvantages of implementing ITIL

However, a disadvantage of ITIL is that it consists of a vast amount of detail and the implementation thereof necessitates training by professional ITIL experts, thus increasing the costs of implementing this control model.

### 3.8.5 The consequences of not complying with ITIL

The following risks are applicable if ITIL is not implemented (ITGI, 2006):

- Support systems will be more prone to errors and may provide unreliable IT systems.
- Inefficient use of resources may be present and business objectives may not be met.

## 3.9 ISO 27001 and ISO 27002

Information has become a company's 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, to thereby provide a competitive advantage to companies.

The ISO 27001 and ISO 27002 standards emphasise the importance of risk management policies and procedures, specifically relating to information security. This includes both IT security systems, and the security of information assets (Carlson, 2008).

The ISO 27001 standard supports the implementation of the ISO 27002 standard. These two standards are usually implemented together in order to ensure a secure information system (Wallhoff, 2004). ISO 27001 forms the foundation of the risk assessment process, whereas ISO 27002 refers to the actual information security controls which are implemented (Maxi-pedia, 2011).

The differences between the ISO 27001 and ISO 27002 standards are discussed in section 3.9.1 and 3.9.2. listed below:

### 3.9.1 ISO 27001 defined

The ISO 27001 standard provides a high level framework for establishing the foundation of the Information Security Management System (ISMS) (Kosutic, 2010). It governs the management controls surrounding the design, implementation, monitoring, maintenance, continuous improvements, and the certification of the ISMS (Maxi-pedia, 2011). ISO 27001 also advises the performance of a risk assessment in

order to identify risk areas and to identify the corresponding ISO 27002 controls which will be implemented to mitigate such risks (Kosutic, 2010).

### 3.9.2 ISO 27002 defined

ISO 27002 (previously known as the ISO 17799 standard) provides a list of operational controls and security considerations which deal specifically with information security matters. The controls listed provide guidance in protecting the information assets, so as to maintain their confidentiality, integrity and availability criteria (Maxi-pedia, 2011). Once the IT strategy and ISO 27001 standard have been established, it is possible to implement the *actual* controls, as listed in the ISO 27002 standard (Kosutic, 2010). ISO 27002 is not a technical standard, but provides a comprehensive minimum baseline of information security controls that should be in place in all information systems (Carlson, 2008). The following areas of controls form the basis of the ISO 27002 standard (Carlson, 2008; ITGI, 2006):

- **Organisational and human resource management:** These areas focus on the control environment determined and communicated by management, establishing the roles and responsibilities of internal and external parties, as well as developing policies and procedures surrounding employing, training and terminating employees.

- **Asset and physical security management:** Strong policies and procedures should be in place in terms of the assignment of responsibilities with regards to the locations and ownership of assets, as well as the protection thereof against physical and environmental hazards.

- **Operations management:** Strong policies and procedures should be implemented over the IT systems, networks and operational processing areas, including the control of all interactions between internal and third parties at information exchange and service delivery levels.

- **Access controls:** Controls should be implemented which will control the access granted to the information assets, by managing the user, network, operating system and application access elements.

- **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 which will identify, respond and manage security incidents. An IT disaster recovery plan should also be developed, in case of emergency situations.

- **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.

Appendix 3 provides a summary of ISO 27002's controls.

### 3.9.3 When to use ISO 27001 and ISO 27002 standards

A company would implement these two standards when it requires reliable information in order to achieve effective decision making processes, as well as to protect sensitive information from unauthorised access (Maxi-pedia, 2011).

### 3.9.4 Advantages of implementing ISO 27001 and ISO 27002 standards

Maxi-pedia (2011) summarises the following advantages specifically applicable to the ISO 27001 and ISO 27002 standards:

- These two standards focus on securing information by preserving the confidentiality, integrity and availability criteria thereof, and thereby protecting the business' information assets.
- The adoption of these standards establishes a risk conscious environment by acknowledging the security risks involved and implementing effective risk management procedures to mitigate such risks.

### 3.9.5 Disadvantages of implementing ISO 27001 and ISO 27002

Carlson (2008) and Sahibudin *et al* (2008) emphasises the fact that the ISO 27001 and ISO 27002 standards do not deal with financial issues, corporate governance,

ethical conduct, or trust issues. The standards only address information security risk management matters.

### 3.9.6 Consequences of not complying with ISO 27001 and ISO 27002

The following risks are present if these standards are not implemented (ITGI, 2006):

- Risk of inappropriate information disclosure,
- Loss of confidence and trust from customers, suppliers and third parties,
- Implementing an inadequate level of risk management due to incomplete risk assessments,
- Inadequate business continuity policies,
- Lack of security awareness within the organisation, including inadequate levels of physical and logical security measures, and
- Inadequate security policies may be in place when interacting with third-party organisations.

By determining a company's business imperatives, and aligning these imperatives to the processes of the control framework, -model and -standard discussed above, good IT governance principles can be achieved at a strategic level.

## 3.10 Access paths

IT governance principles also need to be implemented at an operational level. This is achieved by identifying and assessing the risks of the various access paths which are affected by the specific business imperatives, selected.

### 3.10.1 Access paths defined

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).

### 3.10.2 The components of access paths

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, however the number of actual access paths available is finite (Boshoff, 1990). Each access paths' individual IT architectural components should be identified and examined to ensure that they are correctly built, set up, configured and/or operated, so as to correctly control the particular access path (Boshoff, 2010). These controls are referred to as configuration controls (Santarcangelo, 2010).

## 3.11 Configuration controls

### 3.11.1 Configuration controls defined

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 changes 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 timeously in order to minimise troubleshooting matters (Santarcangelo, 2010).

### 3.11.2 When to implement configuration controls

Organisations depend on their IT assets to process and protect sensitive information. More complex systems could imply a greater exposure to risk and therefore the importance of properly authorised, configured assets increases, especially if the configuration settings on key assets are intentionally or accidentally modified (Santarcangelo, 2010).

### 3.11.3 Advantages of implementing configuration controls

Configuration controls achieve more than completing compliance tick boxes. They provide the following benefits:

- An enterprise is able to add more applications to the system since IT managers have effective oversight in 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 possible due to well managed configuration controls being in place.
- Strong security measures mitigate the relevant risks by ensuring all changes are detected, authorised and documented, lowering compliance costs and resulting in greater efficiency in operations (Tripwire, 2007).

### 3.11.4 Consequences of not implementing configuration controls

An organisation can unintentionally grant access to hackers due to, for example, a misconfigured web server on a critical server or port accidentally being left open on the external router (Santarcangelo, 2010). Assets should therefore be correctly configured. This includes both a company's 'known assets' (the currently 'active' assets IT is aware of) and the 'unknown assets' (the 'inactive/passive' assets which are not active at present or which IT is unaware of). It is important to implement a solution which is able to find and assess a wide variety of assets, whether they are active or passive, and known or unknown in the following areas:

- The entire network and web applications,
- Enterprise applications,
- Middleware and databases, and
- Operating systems and network infrastructures (Santarcangelo, 2010).

## 3.12 Conclusion

These concepts explained above will be used to create an integrated framework in order to 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 ultimately comply with King III's IT governance requirements.

# CHAPTER 4: FINDINGS ON IMPLEMENTING IT GOVERNANCE PRINCIPLES AT A STRATEGIC AND OPERATIONAL LEVEL

## 4.1 An overview of the integrated framework

The integrated framework, shown in Figure 1, depicts the different areas which are affected and are fundamental in establishing such a framework. At a strategic level, companies are driven by their business imperatives. In order to establish and implement strong IT governance principles, the company's business imperatives will be used as its foundation.

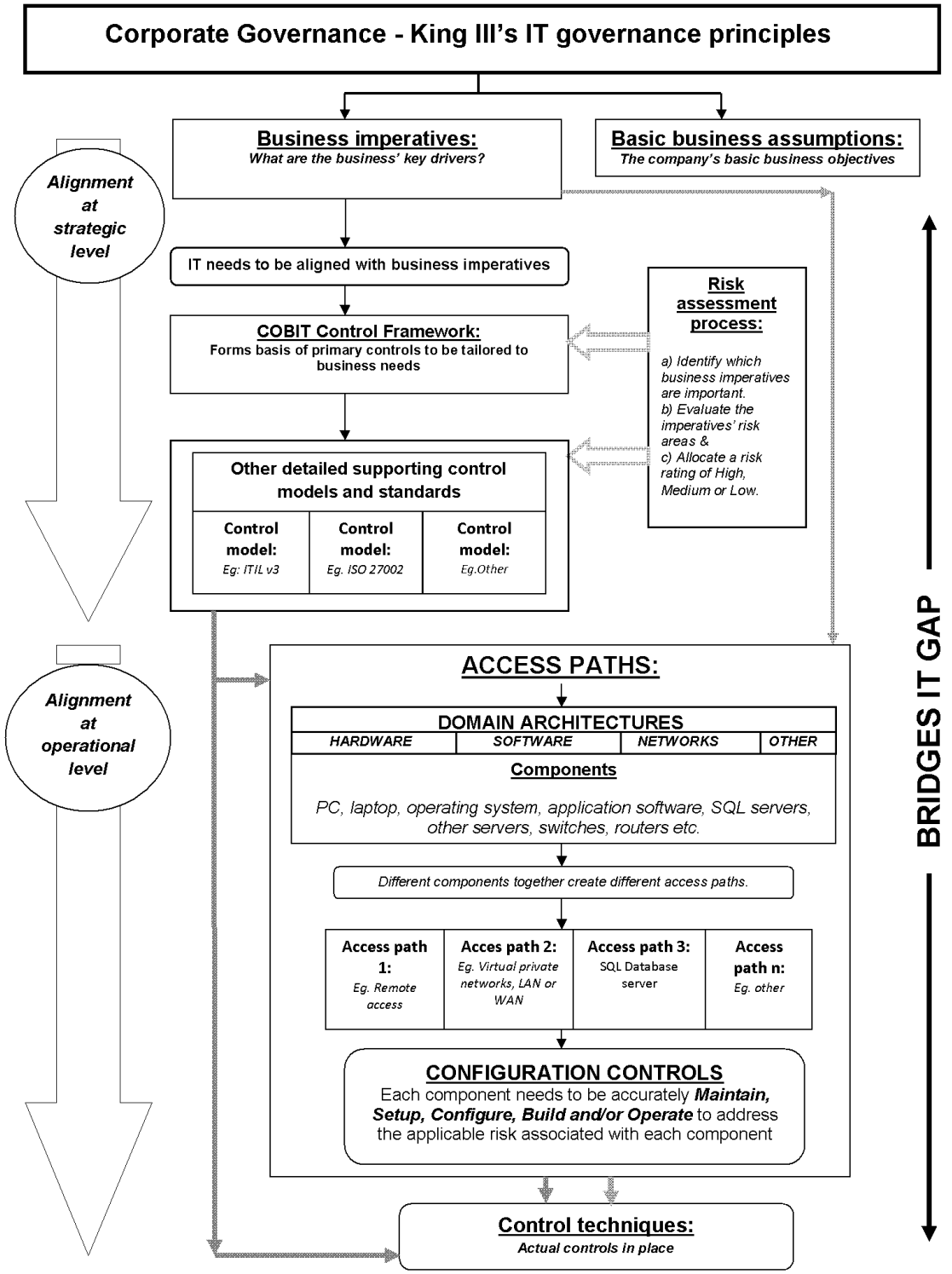
The processes of the COBIT control framework need to be aligned to the chosen business imperatives. The business imperatives' risks are evaluated and the relevant COBIT processes are identified to mitigate these risks. This creates strategic focus in the choice of the controls which are to be implemented. There is therefore no need to simply attempt 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.

The next step will be to align the relevant processes of the ITIL control model and the ISO 27001 and ISO 27002 standards to the processes of the COBIT control framework. By implementing the applicable processes of this control framework, - model and standard above, good IT governance controls can be implemented at a strategic level.

At an operational level, the actual control techniques of the processes identified at the strategic level needs to be implemented. Access paths are also affected by the selected business imperatives. By identifying and evaluating the risks of the access paths and by implementing the relevant configuration controls, IT governance principles will be implemented at an operational level. By implementing these respective controls at both strategic and operational levels, management can ensure that an effective IT governance system is put in place.

This chapter will provide a broad based list of business imperatives which could be applicable to a business environment. In aligning the applicable business imperatives to the processes of the selected control framework, -model and –standard, key control areas was identified which will summarise which IT processes need to be implemented at a strategic level. These key control areas and processes identified above will further be implemented at an operational level, linking it to the relevant control techniques as well as the access paths which are affected by the business imperatives selected. Configuration controls will also be implemented over the components of these affected access paths.

**Figure 1: An integrated framework to align business imperatives with Information Technology governance principles:**



## 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:

### Steps in implementing IT governance at a strategic level:

The following steps should be followed to ensure good IT governance controls at a strategic level:

- Determine a company's business imperatives.
- Evaluate the business imperatives' risks and identify which COBIT processes will appropriately address these risks.
- Link the relevant ITIL and ISO 27002's processes to the selected COBIT processes, which were, in turn linked to the specific business imperatives.

### Steps in implementing IT governance at an operational level:

The following steps should be followed to implement good IT governance controls at an operational level:

i) Implement the applicable control techniques of the relevant processes identified at a strategic level.

ii) Determine the different access paths which are affected by the selected business imperatives.
   - Identify the IT architecture components which form the relevant access paths.
   - Implement relevant configuration controls over each component, ensuring it is either correctly built, maintained, set up or configured, so as to avoid unauthorised access problems.

These above-mentioned steps are explained in more detail below.

### 4.3 Steps in 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 which are applicable to a specific business environment. This research study identified the following 12 business imperatives:

- **Customer service:** Companies often gain a competitive advantage in their environment by ensuring that their customer service levels are superior to those of their competitors. Gathering information provides companies with 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 offer products with only incremental differences between them, companies constantly have to develop new products, so as to address customers' changing needs, retain their loyalty and achieve the competitive advantage. Utilising the research and development department, data mining, collaboration activities, as well as a social media marketing strategy are just a few examples of how innovative ideas can be collected and used in order to develop new products or services (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. Such a system will also provide a company with profit analysis and customer buying trends, and will allow it to determine pinpoint breakeven scenarios, improve product quality and reduce its production and other related costs (Boshoff, 2010; Smit, 2009).

- **Diverse products or business lines:** An information system should be flexible and adaptable enough so as to incorporate diverse product lines, handling each area's costing calculations and production information accurately, and reporting on it in a timely manner. This includes an adaptable system which is 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 such 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 storing and analysing customer, financial and other information. This information is crucial to provide the necessary insight required for decision making processes and to enable a company to gain a competitive advantage in its industry (Smit, 2009). Information can be obtained from data mining, enterprise resource planning (ERP) systems (Smit, 2009), but even more so from today's social media-related interactions, such as blogs and

social networks (Jive Software Company, 2010). These sources of information provide real time information to a company.

- **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. The value chain adds value from the raw material suppliers to the end user activities. 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 a 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).

A company will only select the most important and relevant business imperatives, which are applicable to their business. Once the applicable business imperatives

have been selected, the next step will be to align these business imperatives to the processes of the COBIT control framework.

### 4.3.2 Align the COBIT control framework with the business imperatives

Appendix 4 illustrates the alignment of the relevant COBIT processes with the business imperatives. The alignment between specific business imperatives and its relevant COBIT processes provides a systematic, effective and efficient way in which to start implementing IT controls in a company. A company should select the most appropriate business imperatives, relating to its own company strategies and implement the rest of the integrated framework's guidance based on these chosen business imperatives.

### 4.3.3 Align the processes of the ITIL control model and ISO 27002 standard to the COBIT control framework's processes

Appendix 5 continues to align the processes of the COBIT control framework (originally aligned to the relevant business imperatives as per Appendix 4) to the processes of the ITIL control model and ISO 27002 standard at a high level, summarising the detailed exercise as performed by the ITGI (2008a).

## 4.4 Results of IT governance implementation at a strategic level

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

As discussed in section 4.3, the relevant COBIT, ITIL and ISO 27002 processes were aligned to the business imperatives, which were summarised into a possible 17 key control areas which need to be addressed in order to implement IT governance principles at a strategic level. Based on a company's selected business imperatives, Table 2 shows the applicable key control areas which should be implemented in order to address the business imperatives' specific risk areas and therefore ensure the effective and efficient implementation of IT governance principles at a strategic level.

**Table 2 – 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 processes to the relevant business imperatives**

| Control areas addressed : | Inno-vation | Afford-ability | Diverse products/ Lines | Ease of use | Regulatory compliance | Mobility | Relia-bility | Pro-active management | Collabo-ration | Produc-tivity | Customer service | Repli-cation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | × | | × | | | | | | | | | × |

| **Control areas addressed:** | **Inno-vation** | **Afford-ability** | **Diverse products/ Lines** | **Ease of use** | **Regulatory compliance** | **Mobility** | **Reliability** | **Pro-active management** | **Collabo-ration** | **Produc-tivity** | **Customer service** | **Replication** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | × | | × | × | × | × | × | × | × | | | × |

The key control areas shown in Table 2 above, are discussed below:

**1. Determine business policies and strategies:** 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 ongoing 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. <u>Compliance requirements:</u>** Controls should be implemented so as to adhere to relevant laws and regulations, security policies, technical compliance standards and audit considerations.

**17. <u>Configuration management:</u>** 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.

### 4.4.2 Conclusion on IT governance implementation at a strategic level

A company should identify those specific business imperatives which are applicable to its business. These business imperatives will form the foundation of implementing IT governance principles at a strategic level. Management can now consult Table 2 to determine which *high level* key control areas need to be addressed so as to mitigate the risks associated with the specific business imperatives selected. 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.

## 4.5 Steps in implementing IT governance at an operational level

### 4.5.1 Implement the IT control framework, -model and –standards' control techniques

In order to physically implement the actual control techniques, of those key control areas summarised in Table 2 above, a company will:

i) Identify their specific business imperatives.
ii) Thereafter, consult Appendix 4 to determine which COBIT processes are applicable, based on the selected business imperatives, and
iii) Implement the actual controls listed in Appendix 5, which are shown per applicable COBIT process and controls, linked to the ITIL and ISO 27002 controls. The detail of these controls can be found in the applicable Appendices 1,2 or 3 depending on which framework, model or standard are being referred to.

### 4.5.2 Access paths, access paths' components and configuration controls

- **Determine the relevant access paths:** 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 affects different access paths. All such possible access paths should be identified and risk managed.

  Each access path consists of various IT architecture components, which, when used together, form an access path. Each of these different components should be identified, risk assessed and controlled, by implementing the appropriate configuration controls. Together, these components form access paths by creating a LAN (Local Area Network), a WAN (Wide Area Network), a remote access port, a VPN (Virtual Private Network) connection, or any other connection.

- **Control the risks of access paths:** The relevant access paths and their components are determined in order to prevent unauthorised use or access to the enterprise's data and functions via an unprotected or incorrectly set up access path (Boshoff, 1990). Different access paths will apply for different users, based on each user's access rights, restrictions, user profile and terminal identification settings (Boshoff, 1990). Multi-domain environments often have a large number of primary accessors and activities, and hence various different access paths. Certain activities, classified as public domain areas, might require no or little security measures, whilst others may require a very high degree of security. It is therefore impractical to secure all areas to the highest level. Depending on the circumstances and risks involved, it is now possible to differentiate among access paths and apply the appropriate level of security to such risks (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 ups, the *technology* level is risk managed.

  The risk exists that inappropriate access path set ups may have been established for existing users, allowing them to access known access paths. However an additional risk

exists that unactivated access paths may exist which IT is unaware of. An unactivated access path may contain unactivated accessors, which can be accessed by third parties and other unauthorised users, since no relevant controls have been implemented over such access paths (Boshoff, 1990). This exposes a company to an intolerable high level of risk. In order to avoid risk levels becoming too high, all relevant access paths should be adequately managed through the appropriate setting up of configuration controls.

- **Manage the set up of IT components:** Each access path's individual IT architectural components (being specific hardware, software, network and other applicable parts) should be identified to ensure that they are either correctly *built, set up, configured* and/or *operated* (known as configuration controls) so as to correctly control the particular access path (Boshoff, 2010).

The configuration controls are defined as follows below:

- 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 also '*built',* referring either to the process of creating and converting source code files into stand-alone software artefacts that can be run on a computer, or the result of doing so. This will include the compilation process, where source code files are converted into executable code (Boshoff, 2010).

- *'Set up'* or '*installation'* of a program (including drivers, plugins, etc.) refers to implementing the program on a computer system and ensuring the execution thereof (Boshoff, 2010).

- 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 (Boshoff, 2010).

- 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 (Boshoff, 2010).

- *'Maintenance'* ensures that software is upgraded and/or computers/devices are repaired so as to ensure the optimum performance and reliability of such devices (Boshoff, 2010).

If correctly implemented, these configuration controls and the relevant IT components will address the risks surrounding the access paths. These configuration controls also need to be independently reviewed, properly documented as well as any other relevant control techniques implemented that is applicable in controlling the risks of these access paths.

### 4.5.3 Conclusion on IT governance implementation at an operational level

Implementing the control techniques at an operational level normally addresses the corresponding risks, identified at this level. However, incorrect access path configuration settings represent an additional risk area, which is normally overlooked and not appropriately addressed. Ensuring a system's configuration settings remain compliant with internal security and compliance policies remains a significant challenge for any organisation (Santarcangelo, 2010). Configuration controls complete the risk assessment process, enhancing the visibility of assets on the network with specific benefits to operations, audit and security matters (Santarcangelo, 2010).

## 4.6 Align the business imperatives to the IT governance principles at a strategic and an operational level

Appendix 6 shows the mapping performed between the COBIT processes (which was mapped to the ITIL and ISO 27002's processes in Appendix 5) and the relevant King III principles and key international IT governance areas. Appendix 7 link these results back to the business imperatives' relevant COBIT processes (alignment performed in Appendix 4). This confirms that by using business imperatives as a starting point in the implementation of the integrated framework, the King II's IT governance principles as well as the international IT governance areas are achieved at both a strategic and operational level.

## 4.7 Conclusion

The effective and efficient implementation of IT governance principles has been achieved by focusing on the relevant risk areas, based on the business imperatives which affect both the strategic and operational business levels. By implementing the relevant IT key control areas provided in Table 2 and the detailed control techniques listed in Appendix 5, the key risk areas will be addressed at both a strategic and operational level. The business imperatives selected also affect certain access paths at an operational level which will be controlled through the implementation of configuration controls.

By using business imperatives as a foundation for implementing strong IT controls, it was shown and confirmed in Appendices 6 and 7 that King III's IT governance principles are in fact managed and addressed at both a strategic and operational level. By using the guidance provided by the developed integrated framework, it is no longer necessary to simply complete compliance questionnaires without having a strong foundation in choosing controls. Businesses are no longer seen as carrying one generic risk profile, but key risk areas can now be identified and addressed, based on a company's business imperatives, which address risks at both a strategic and operational level in an effective manner, whilst complying with IT governance requirements.

# CHAPTER 5: CONCLUSION

Greater responsibility has been placed on directors and management for the implementation of IT governance principles. However, most management do not understand the concepts surrounding IT governance and implement the processes of IT control frameworks, -models and –standards in an ad hoc manner, resulting in an ineffective IT governance system being implemented.

The aim of this study was to develop an integrated framework in order to effectively implement IT governance principles. IT governance principles should first be implemented at a strategic level by implementing the relevant processes of the best practice IT control framework, -model and -standard, based on a company's business imperatives. The second level of implementing IT governance principles is the operational level, which refers to implementing the relevant control techniques as well as addressing the relevant access path risks. The following steps form the basis of the developed integrated framework:

- **Step 1:** At a strategic level, specific and applicable business imperatives of a company should be identified.
- **Step 2:** By consulting Table 2, the relevant key control areas, based on the selected business imperatives, can be identified as to address the IT risks at a strategic level.
- **Step 3:** At an operational level, management should implement the key areas' control techniques, as identified in step 2 above.
- **Step 4:** The relevant access paths and its components, which are affected by the selected business imperatives, should also be identified and assessed for risks.
- **Step 5:** Configuration controls should be implemented over these components in order to address the risks surrounding these areas.

Since this study did not focus on providing the detailed guidance surrounding the implementation of the control techniques, the access path identification process or providing guidance on how to practically implement configuration controls, these areas remain available for further research studies.

The above-mentioned steps do however provide practical guidelines which can be used by senior management and directors in identifying and addressing the relevant and critical IT risk areas of a company. By implementing the developed integrated framework, the company will ensure that it complies with King III's IT governance principles at both a strategic and operational level.

# REFERENCES


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.

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. 1990. A path context model for computer security phenomena in potentially non-secure environments. Unpublished doctoral dissertation. Johannesburg: Rand Afrikaans University.

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: http://www.orangeparachute.com/documents/Understanding_ISO_27002.pdf. Accessed: 6 January 2011.

Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I., Windebank, J. & Rance, S. 2007. An introductory overview of ITIL V3. Online: http://www.itsmfi.org/files/itSMF_ITILV3_Intro_Overview_0.pdf. Accessed: 2 February 2011.

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.

Cherry Tree & Company. 2000. Extended Enterprise applications. Online: http://www.sysedv.tu-berlin.de/intranet/kc-kb.nsf/bc64cc33c3daf5fec1256979005bc026/F16DB8D8AA21A63DC1256CD300398C69/$File/Extended+Enterprise+Applications.pdf?OpenElement. Accessed: 23 August 2011.

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: http://www.isaca.org/Journal/Past-Issues/2005/Volume-2/Documents/jopdf052-IT-Gov-Pass-or-Fail.pdf. Accessed: 3 August 2011.

Drury, C. 2004. *Management and Cost Accounting* (6th ed.). London: Thomson Learning.

Hardy, G. 2006a. Guidance on aligning COBIT, ITIL and ISO 17799. Online: http://www.isaca.org/Journal/Past-Issues/2006/Volume-1/Documents/jpdf0601-Guidance-on-Aligning.pdf. Accessed: 5 January 2011.

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: http://www.vpit.ualberta.ca/frameworks/pdf/itil_cobit.pdf. Accessed: 18 January 2011.

IBM. 2006. Igniting innovation through business and IT fusion. Online: http://www-935.ibm.com/services/fr/cio/flexible/flex_wp_gts_fusion_business_it.pdf. Accessed: 4 August 2011.

IBM. 2009. Coming to grips with enterprise IT. Online: ftp://ftp.software.ibm.com/software/tivoli/analystreports/coming-to-grips-ITILv3.pdf. Accessed: 23 August 2011.

Innotas. 2010. The CXO's guide to IT governance. A roadmap to driving top-down alignment between business & IT strategy. Online:

http://solutioncenters.cio.com/innotas_governance/registration/5962.html?source=ciozne. Accessed: 20 May 2011.

Institute of Directors Southern Africa (IODSA). 2009. King Report on corporate governance for South Africa (King III). Online: http://www.iodsa.co.za. Accessed 3 August 2011.

IT Governance Institute. 2006. COBIT mapping: Overview of international IT guidance, 2nd edition. Online: http://www.sox-expert.com/uploads/files/COBIT%20Mapping%202nd%20Edition.pdf . Accessed: 23 August 2011.

IT Governance Institute. 2007. COBIT 4.1. Online: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-4-1.aspx. Accessed: 25 November 2010.

IT Governance Institute. 2008a. Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for business benefit. Online: http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT,ITILV3,ISO27002-Bus-Benefit-12Nov08-Research.pdf. Accessed: 8 December 2010.

IT Governance Institute. 2008b. COBIT Mapping. Mapping of ITIL v3 with COBIT 4.1. Online: http://www.itsm.hr/baza%20znanja/Mapping%20ITILV3%20COBIT41.pdf. Accessed: 1 September 2011.

IT Governance Institute. 2008c. Understanding how business goals drive IT goals. Online: http://www.isaca.org/Knowledge-Center/Research/Documents/Understand-Bus-Drive-IT-Goals-15Oct08-Research.pdf. Accessed: 18 October 2011.

Jive Software Company. 2010. The 18 social business imperatives. Online: http://www.jivesoftware.com/files/pdf/whitepaper/WP-18BusinessImperatives-JiveSoftware.pdf. Accessed: 23 September 2011.

Johnston Turner, M., Oltsik, J. & McKnight, J. 2009. ISO, ITIL & COBIT together foster optimal security investment. Online: http://www.thecomplianceauthority.com/iso-itil-a-cobit.php. Accessed: 20 May 2011.

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

Kosutic, D. 2010. ISO 27001 vs ISO 27002. Online: https://www.infosecisland.com/blogview/8055-ISO-27001-vs-ISO-27002.html. Accessed: 23 August 2011.

Liell-Cock, S., Graham, J. & Hill, P. 2009. IT governance aligned to King III. Online: http://lgict.org.za/sites/lgict.org.za/files/documents/2009/liell-cock-graham-hill-2009-it-governance-aligned-king-iii.pdf. Accessed: 20 Junie 2011.

Maxi-Pedia Encyclopedia. 2011. ISO 27001. Online: http://www.maxi-pedia.com/ISO+27001. Accessed: 23 August 2011.

McRitchie, J. 1999. Corporate Governance. Online: http://www.corpgov.net/library/definitions.html. Accessed: 9 June 2011.

Muller, R. 2009. IT governance report slated. Online: http://mybroadband.co.za/news/general/7242-it-governance-report-slated.html. Accessed: 3 Aug 2011.

Numara Software. 2009. Show me the money. How life in the ITIL fast lane can deliver success. Online: http://www.findwhitepapers.com/whitepaper7394. Accessed: 20 May 2011.

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: http://www.accountancysa.org.za/resources/ShowItemArticle.asp?ArticleId=1398&Issue=979. Accessed: 22 September 2011.

Rudman, R.J. 2008b. IT governance: a new era. *Accountancy SA*. March 2008: 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. *Second Asia International Conference on Modelling & Simulation, 2008.* Online: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4530569 Accessed: 29 November 2010.

Santarcangelo, M. 2010. Configuration auditing – the next critical step in compliance. Online: http://www.thecomplianceauthority.com/compliance-whitepapers/configuration-auditing-next-critical-step-in-compliance.pdf. Accessed: 20 May 2011.

Simkova, E. & Basl, J. 2006. Business value of IT. Online: http://si.vse.cz/archive/proceedings/2006/business-value-of-it.pdf. Accessed: 22 September 2011.

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.

The Economist. 2006. Great expectations: The changing role of IT in the business. September 2006. Online: http://graphics.eiu.com/ebf/PDFs/GTF_article_1_September_06_FINAL.pdf. Accessed: 22 September 2011.

Tripwire Incorporated. 2007. Winning the IT Control game: using configuration audit and control to improve efficiency and control risk. Online:

http://www.aservo.com/fileadmin/user_upload/downloads/tripwire/Tripwire_Winning_the_IT_Control_Game_WP.pdf. Accessed: 23 May 2011.

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: http://www.accountancysa.org.za/resources/ShowItemArticle.asp?ArticleId=2044&Issue=1097. Accessed: 22 September 2011.

Wallhoff, J. 2004. Combining ITIL with COBIT and ISO/IEC 17799:2000. Online: http://www.scillani.se/assets/pdf/Scillani%20Article%20Combining%20ITIL%20with%20Cobit%20and%2017799.pdf. Accessed: 26 November 2010.

# APPENDICES

**Appendix 1: COBIT control framework and processes**

The following summary of the COBIT processes were documented by ITGI (2007) and Smit (2009).

**Appendix 2: ITIL control model and processes**

The following areas form the basis of implementing ITIL processes and service management controls, as described by ITGI (2006),ITGI (2008b) and Cartlidge *et al* (2007).

**Appendix 3: ISO 27002 standard and controls**

The ISO 27002 controls were summarised by Carlson (2008) and ITGI (2006).

**Appendix 4: COBIT processes aligned with the business imperatives**

Appendix 4 reflects the alignment exercise performed between the business imperatives and the relevant COBIT processes.

**Appendix 5: Mapping between the COBIT control framework, ITIL control model and ISO 27002 standard's processes**

According to ITGI (2008a) a mapping has been performed between the above mentioned control framework, -model and -standard.

**Appendix 6: Align the COBIT processes to the international IT governance key areas and King III's IT governance principles**

The COBIT processes were aligned to the key international IT governance areas and King III's IT governance principles.

**Appendix 7: Align business imperatives to the international IT governance key areas and King III's IT governance principles**

The relevant COBIT processes and its results as shown in Appendix 6, were aligned with the applicable business imperatives as shown in Appendix 4, achieving an alignment between business imperatives, its COBIT processes, key international IT governance areas and King III's IT governance principles.

**Appendix 1: COBIT control framework and processes**

| Nr | COBIT domain | Process | Description of controls |
|---|---|---|---|
| 1. | **Plan and Organise (PO)** | PO1: Derive a strategic IT plan | Plan IT resources optimally in order to meet business objectives and strategies, by performing accurate resource management procedures. |
| | | PO2: Define the information architecture | IT function should produce and frequently update the IT architecture of the business information model in order to ensure the data maintains its integrity, security and improve quality of management's decision-making abilities. Information sharing should remain flexible, cost effective, timely and secure. This domain includes data management procedures such as: data ownership, retention, appropriate classification of data, encryption and archiving. Integrity management policies and procedures are also included, which relate to activities that ensure the integrity and consistency of all data in electronic form, such as databases, database warehousing and data archiving actions. |
| | | PO3:Determine the technological direction | Existing and emerging technologies should be investigated and determine which technologies will create business opportunities and realise business and IT strategies. The design of an IT infrastructure plan includes matters such as managing system's architecture, IT strategic direction, acquisition procedures, standards, migration approaches, analysing trends and consider regulatory compliance standards as well as incident and security management procedures. |
| | | PO4:Define IT processes, organisation & relationships | Define IT processes and functions as well as determine IT staff's organisational structure. Relationships between business and IT management include setting up strategy and steering committees. Consideration should also be given to staff skills, functions, accountability, authorisation structures, roles and responsibilities, supervision and third-party agreements by implementing the relevant risk management, quality assurance and security controls. |

| Nr | COBIT domain | Process | Description of controls |
|---|---|---|---|
| | | PO5: Manage IT investments | The IT investment programme should manage costs, profits, budgets, cost versus benefit analyses, return on investments and the effective and efficient use of IT resources. |
| | | PO6: Communicate management aims and direction | Management should set a strong control environment in place, communicating its IT control framework, which includes the understanding of business and IT risks, the business' objectives and direction. This ensures achieving IT objectives and complying with relevant laws and regulations. |
| | | PO7: Manage IT human resources | Appropriate procedures in terms of recruiting, training, evaluating, promoting and terminating of IT staff should be put in place. |
| | | PO8: Manage quality | A quality management systems (QMS) should be developed and maintained consisting of approved development and acquisition processes and standards. A QMS ensures IT delivers value to the business, continuously improving quality standards and communicates results to shareholders in a transparent manner. |
| | | PO9: Assess and manage IT risks | A risk management framework should be developed, which includes agreed-upon level of IT risks, its mitigation strategies and the level of residual risks tolerated. |

| Nr | COBIT domain | Process | Description of controls |
|---|---|---|---|
| | | PO10: Manage projects | Develop a programme and project management framework, which manages all IT projects. The framework will ensure the right prioritisation and co-ordination of the projects, including its resource allocations, list of deliverables defined, user approval, phased delivery approach, quality assurance, a formal test plan and post-implementation reviews. |
| **2.** | **Acquire and implement (AI)** | AI1: Identify automated solutions | Before a new application is required or developed, an analysis should be performed to ensure the business's needs are met by considering the following aspects: alternative sources, its technological and economic feasibility study, identifying the risk areas and performing a cost versus benefit analysis. |
| | | AI2: Acquire and maintain application software | The design of an application is made available in line with business requirements, implementing the appropriate applications controls, ensuring the development and configuration levels are in line with the relevant standards. |
| | | AI3: Acquire and maintain technology infrastructure | Formal processes and internal controls should be in place to acquire, implement and upgrade the business's technology infrastructure. Internal controls should be in place with regards to the configuration, integration and maintenance of hardware and software components, protecting the resources' availability and integrity. A test environment must also be setup to perform integration tests on these infrastructure components. |

| Nr | COBIT domain | Process | Description of controls |
|---|---|---|---|
| | | AI4: Enable operation and use | Communicate knowledge with regards to new systems to staff and employees via documentation, manuals and providing the appropriate training. |
| | | AI5: Procure IT resources | A formal procurement process should be implemented in order to procure the correct people, hardware, software and supplier services in a cost-effective and timely manner. |
| | | AI6: Manage changes | All changes made to infrastructure and applications should be formally managed. All changes should be recorded, evaluated and authorised before implementation and assessed against the planned outcomes. |
| | | AI 7: Install and accredit solutions and changes | Perform detailed testing on new systems in a dedicated environment by making use of test data. The implementation, migration and release procedures should be established as well as performing post-implementation reviews on such systems. |
| **3**. | **Deliver and support (DS)** | DS1: Define and manage service levels | The business users and IT management should establish and document which IT services and service levels are required. This ensures alignment between the IT services rendered and the business' requirements. |

| Nr | COBIT domain | Process | Description of controls |
|---|---|---|---|
| | | DS2: Manage third-party services | Effective third-party agreements should be in place in order to define the roles, responsibilities and expectations of third parties. Such agreements should be reviewed and monitored ensuring business requirements are met. |
| | | DS3: Manage performance and capacity | Review the present performance and capacity of IT resources, taking into account forecasts of future required business needs and its related IT resources needed. |
| | | DS4: Ensure continuous services | Providing continuous IT services requires the development, maintenance and testing of IT continuity plans, off-site backups and providing periodic continuity training. |
| | | DS5: Ensure system security | Security management processes should be implemented, maintaining information's integrity and protecting IT assets. The establishment of IT security roles and responsibilities, policies, standards and procedures should be in place. Activities include: performing security monitoring and periodic testing, implementing corrective actions and identifying security weaknesses and incidents. |
| | | DS6: Identify and allocate assets | Implement a system which measures, allocates and reports IT costs accurately to the users of the services, linking the costs to a specific business process. |
| | | DS7: Educate and train users | Train all IT users in order to minimise user errors, enhance productivity and increase compliance with key controls. |

| Nr | COBIT domain | Process | Description of controls |
|---|---|---|---|
| | | DS8: Manage service desk and incidents | Implement a service desk and incident management process so as to timely and effectively respond, analyse and resolve IT user queries and problems. |
| | | DS9: Manage configurations | An accurate and complete configuration repository should be created, to establish initial hardware and software configurations, verify and audit configuration information and update the repository as needed. |
| | | DS10: Manage problems | A problem management system should be implemented, which identifies, classifies, analyses and resolves problems. |
| | | DS11: Manage data | Implement effective data management processes via managing the media library, backups and recovery of data and proper disposal of media, which will result in quality, timely and available business data. |
| | | DS12: Manage physical environment | Well-designed and well-managed physical facilities should be established in order to ensure adequate protection of computer equipment and personnel, including monitoring environmental factors and managing the physical access to such areas. |
| | | DS13: Manage operations | Data management and hardware maintenance procedures should be put in place in order to ensure the complete and accurate processing of data. |

| Nr | COBIT domain | Process | Description of controls |
|---|---|---|---|
| **4.** | **Monitor and Evaluate (ME)** | ME1: Monitor and evaluate IT performance | An effective IT performance management system should be implemented which defines relevant performance indicators, systematic and timely reporting of performances and prompt responses to deviations. |
| | | ME2: Monitor and evaluate internal control | Establish a well-defined efficient internal IT control programme. This programme will include monitoring and reporting on control errors, self-assessment results and third-party reviews, as well as complying with applicable laws and regulations and gaining assurance on effective and efficient operations. |
| | | ME3: Ensure compliance with external requirements | A review process needs to be implemented in order to ensure compliance with the relevant laws, regulations and contractual requirements. |
| | | ME4: Provide IT governance | Establishing an effective governmental framework which defines the organisational structures, processes, leadership, roles and responsibilities in order to ensure that the enterprise's IT investments are aligned and delivered in accordance with the enterprise's strategies and objectives. |

**Appendix 2: ITIL control model and processes**

| Nr | Key area | Process | Description of controls |
|---|---|---|---|
| **1.** | **Service Strategy (SS)** | 1. Determine the business service requirements and market share | Determine existing and potential customer needs, the current and potential markets, the service provider's competitors and how the IT services will add value to the business. |
| | | 2. Determine IT policies and strategies | **2.1 Organisational level:** Develop an organisational structure with the appropriate level of IT controls in place and develop and create an IT risk averse culture among employees and third parties.<br>**2.2 Operational level:** Implement IT tactical plans and an IT process framework by implementing a service level management framework, defining all related services and the processes it relate to.<br>**2.3 Technological level:** manage the elements of service automation and service interfaces by defining the business functional areas and its corresponding technical requirements as well as controlling the configuration settings of IT components. |
| | | 3. Financial management for IT services and return on investments | This area manages the processes relating to the IT service provider's budgeting, accounting and charging requirements as well as the financial value and return on IT investments (IT services and IT architecture components). It also ensures accurate and reliable accounting data is available for decision-making procedures. IT related expenses should be managed by creating cost centres which accurately allocate costs to functional process areas and perform IT budget versus actual IT costing analysis. |

| Nr | Key area | Process | Description of controls |
|---|---|---|---|
| | | 4. Service portfolio management | Implement proactive management procedures with regards to the IT investments, including managing those services delivered in the concept, design, transition, service catalogues and retired phases. Customers' supply and demand for services should be aligned, prioritised and balanced by authorising and allocating services and resources appropriately. |
| | | 5. Demand management | Understand and influence customers timing in demanding services and provide the appropriate capacity to meet these demands on a strategic and tactical level. |
| | | 6. Risk management | Develop an IT risk management framework in order to identify and manage the relevant IT risks. |
| **2**. | **Service Design (SD)** | 1. Service design aspects | This area covers the design and development aspects of IT services which includes the design and development of:<br>1.1 The business service requirements and business service management systems.<br>1.2 The development and acquisition standards.<br>1.3 The service solutions and service portfolios.<br>1.4 The IT architecture structures.<br>1.5 The IT processes.<br>1.6 The measurement of systems and its required criteria.<br>1.7 The evaluation of alternative solutions and procure the correct solution and<br>1.8 The determination of the design constraints of the solution. |

| Nr | Key area | Process | Description of controls |
|---|---|---|---|
| | | 2. Service Level Management (SLM) | The goal of SLM is to ensure all operational services rendered comply with the services demanded and agreed upon. The services delivered should be measured in a consistent and professional manner throughout the IT organisation. It will include activities such as:<br>• Identifying users and manage internal and external suppliers.<br>• Developing internal operational and supplier level agreements.<br>• Monitoring and improving service quality levels.<br>• Dealing with complaints and compliments accordingly, so as to enhance customer satisfaction levels. |
| | | 3.Service Catalogue Management (SCM) | The purpose of SCM is to provide a single document in which it is recorded and agreed upon which IT services are to be rendered. |
| | | 4. Supplier management | The purpose of the Supplier Management process is to select the appropriate suppliers, obtain valued services from such suppliers and to ensure that suppliers comply with their agreed-upon services and signed contracts. Supplier risk management procedures should also be in place. |
| | | 5.Capacity Management (CM) | The goal of CM is to proactively identify the current and future performance requirements of users and match the capacity of IT to these agreed current and future business demands by managing and allocating the appropriate resources. |

| Nr | Key area | Process | Description of controls |
|---|---|---|---|
| | | 6. Availability management | The purpose of Availability Management is to manage matters relating to available services, components and resources, ensuring that they match or exceed the current and future needs of the business in a cost-effective and timely manner. |
| | | 7. IT security management | The focus of IT security management is to ensure that data maintains its availability, confidentiality, integrity, authenticity and non-repudiation criteria. These criteria are maintained by implementing an IT security plan, performing appropriate risk assessments, establishing a well–secured IT environment, incident identification, the handling of such incidents and developing and implementing the appropriate service level management framework. The IT security goals should be aligned to the business security goals. |
| | | 8. IT service continuity management (ITSCM) | The purpose of ITSCM is to maintain the appropriate on-going recovery capability within IT services to match the agreed needs, requirements and timescales of the business, as well as remaining aligned with business continuity plans. Risk assessment procedures are also necessary to identify the relevant risks, the appropriate responses and ensure IT continuity plans and off-site backup storage facilities are in place. |
| | | 9. Data and information management | Develop an enterprise architecture model including a data dictionary and a data classification scheme. An integrity management system should also be implemented ensuring the integrity and consistency of all data stored electronically. Data management, storage, retention, policies and procedures should be in place. |

| Nr | Key area | Process | Description of controls |
|---|---|---|---|
| | | 10. Application management | Application Management focuses on software development using a life-cycle approach, as well as the system design, acquisition and changes made based on clear user requirements. |
| | | 11.Organisational management | This area identifies the relevant individual functional areas, its related activities, as well as the relevant staff's roles, responsibilities and skills. |
| | | 12. Technological considerations | Guidelines are provided on establishing the data dictionary and syntax rules, service orientated architecture policies, development and acquisition standards, as well as developing the appropriate technological policies, plans and procedures. |
| | | 13. Service design implementation | Perform a business risk impact analysis including the risks surrounding the service and process levels as well as implementing and measuring the service designs chosen. |
| **3.** | **Service Transition (ST)** | 1. Service transition policies | Establish a formal service transition policy through which all changes are managed and implemented. Such policies should address the company's transition requirements and establish good relationships with the stakeholders. A control framework and set standards should be implemented, in order to manage the quality of changes made to the system. |

| Nr | Key area | Process | Description of controls |
|---|---|---|---|
| | | 2. Service transition, planning and support | A reliable transition and change management system should be established in order to standardise all changes made to applications, procedures, processes, systems and configurations. It should also control the risk of failures and disruptions across transition activities by identifying all changes made and reporting on irregular changes. The resources should also be planned and coordinated in order to ensure that the business and user requirements are effectively realised. An effective communication policy should be implemented as well as full commitment and support from management and all stakeholders involved. |
| | | 3. Change management | Change management will include the request for changes logged, the assessment, review and authorisation of such changes. It includes both normal and emergency type changes to be made. Changes need to be authorised by the change advisory board. It will also include activities such as the addition, modification or removal of an authorised, planned or supported service or service component and its associated documentation. |
| | | 4. Organisational management | Determine the organisational structure of the company, including<br>1.1 the roles and responsibilities to support the transition processes<br>1.2 the change standards, policies and procedures |

| Nr | Key area | Process | Description of controls |
|---|---|---|---|
| | | 5. Service asset and configuration management (SACM) | The purpose of SACM is to identify, control and account for service assets and configuration items (CI), protecting and ensuring their integrity across the service life-cycle. The scope of SACM also extends to non-IT assets and to internal and external service providers, where shared assets need to be controlled. Strict configuration management is essential and will include the following activities:<br>• Accounting for IT assets and configurations.<br>• Identifying and labelling sound configuration items.<br>• Verifying the configuration records and correct exceptions.<br>• Identifying sound configuration procedures by implementing controls which will ensure that only authorised and identifiable configuration items are recorded. |
| | | 6. Release and deployment management | It covers the whole assembly and implementation of new or changed services for operational use, from release planning through to early life support. Only tested, approved and accredited components (hardware, software, firmware and documents) and applications are installed error-free and on schedule, providing training to users and perform pre-and post implementation reviews. |
| | | 7. Knowledge management | The purpose of Knowledge Management is to ensure that the right person (whether it is management, users or operational staff) has the right knowledge, at the right time to deliver and support the services required by the business, which will result in improved and more efficient quality services. The core of Knowledge Management is the Data-Information-Knowledge-Wisdom structure, condensing raw and unusable data into valuable assets. |

| Nr | Key area | Process | Description of controls |
|---|---|---|---|
| | | 8.Service validation, testing and implementation | The key purpose of this area is to test the new or changed services implemented in order to ensure it support the business requirements and service levels include the agreed service level agreements (SLAs). |
| | | 9. Evaluation | Evaluate relevant areas in order to identify, assess and respond to relevant risk areas and determine its impact on the business. |
| **4.** | **Service Operation (SO)** | 1. Service operation policy | Establish formal policies and procedures describing the different functional areas and processes across the life-cycle through the implementation of a formal IT process framework. |
| | | 2. Event management | This area includes the notification and detection of events (non-routine problems) which occur and how to address such events by implementing the appropriate risk response procedures. It also includes monitoring the status of components, even when no events have occurred. |
| | | 3. Access management | The purpose of this process is to verify and provide the appropriate users with the correct level of access rights, monitor and log access routes and remove or restrict rights to unauthorised users. It helps to manage and maintain the confidentiality, availability and integrity of data and intellectual property. |

| Nr | Key area | Process | Description of controls |
|---|---|---|---|
| | | 4. Incident management | An incident is an unplanned interruption to an IT service, or a reduction in the quality of an IT service. The purpose of Incident Management is to efficiently and effectively restore normal service as quickly as possible, and to minimise the adverse impact on business operations. It includes the identification, logging, categorisation, prioritisation, diagnosis, investigation and correction of incidents. |
| | | 5. Request management | The purpose of Request Management is to authorise the appropriate users to request and receive standard services, to deliver these services, to provide information to users about services and procedures and to assist with general information, complaints and comments. A service request is a user request for information, advice, a standard change, or for access to an IT service. |
| | | 6. Organisational management | Develop an organisational structure which includes segregating staff's roles and responsibilities in each different functional area, teams and departments. Management service levels should also be established. Communicate and document the IT objectives and direction of the company. |

| Nr | Key area | Process | Description of controls |
|---|---|---|---|
| | | 7. Problem management | The key objectives of Problem Management are to detect, log, categorise, prioritise, investigate, diagnose and resolve problems and its resulting incidents. It should also eliminate recurring incidents and minimise the impact of incidents that cannot be prevented. The following sub-categories are part of the problem management area:<br>**7.1 Service Desk Function:** The Service Desk provides a single central point of contact for all IT users. It logs and manages all incidents, service and access requests.<br>**7.2 Technical Management Function:** Technical Management includes all the people who provide technical expertise and management of the IT infrastructure. Technical Management helps to plan, implement and maintain a stable technical infrastructure and ensure that required resources and expertise are in place to design, build, transition, operate and improve the IT services and supporting technologies.<br>**7.3 Application Management Function:** Application Management includes all the people who provide technical expertise and management of applications. Their focus is on software applications rather than infrastructure matters.<br>**7.4 IT Operations Management Function:** IT Operations Management is responsible for the management and maintenance of the IT infrastructure required to deliver the agreed level of IT services to the business. |

| Nr | Key area | Process | Description of controls |
|---|---|---|---|
| | | 8. Common service operation activities (CSO) | CSO includes a number of activities that are not part of the five processes described. These include:<br>**8.1 Monitoring and control:** detect the status of services and configuration items and take appropriate corrective action.<br>**8.2 IT operations:** a central coordination point for managing services whilst monitoring IT infrastructure components.<br>**8.3 Infrastructure management:** off-site backup storage facilities should be implemented and preventative maintenance done on mainframe and hardware components. It also includes the management of servers, networks, database administration setups, information security systems, middleware, internet, data centres and directory services.<br>**8.4 Processes' operational aspects from other life-cycle stages:** Change, configuration, release and deployment, availability, capacity, knowledge, financial and service continuity management principles. |
| | | 9. Service operations' implementation | Implement the IT process framework in order to implement effective and efficient operational functional areas. |
| **5.** | **Continual service improvement (CSI)** | 1. CSI policies and procedures | Develop an IT governance framework, determining the standards and quality systems, the organisational structures and roles and responsibilities that need to be in place in the CSI cycle. |

| Nr | Key area | Process | Description of controls |
|---|---|---|---|
| | | 2. Seven step improvement process | **Step 1 - Define what one should measure:** identify what is needed to fully satisfy the goals, without considering whether the data is currently available.<br>**Step 2 - Define what one can measure:** A gap analysis should be conducted between what is or can be measured today and what is ideally required. The gaps and implications are then reported to the business, the customers and IT management.<br>**Step 3 - Gather the data:** This covers the monitoring and data collection processes.<br>**Step 4 - Process the data:** Raw data is processed into the required format, typically providing an end to-end perspective on the performance of services and/or processes.<br>**Step 5 - Analyse the data:** Data is analysed and transformed into knowledgeable and meaningful information and results.<br>**Step 6 - Present and use the Information:** The knowledge gained is presented in a format easily understood and allows those receiving the information to make strategic, tactical and operational decisions. It should provide value, note service exceptions and highlight any benefits that have been identified during the time period.<br>**Step 7 - Implement corrective action:** The knowledge gained is used to optimise, improve and correct services, processes, and other supporting activities and technology. The corrective actions required to improve the service should be identified and communicated to the organisation. |

| Nr | Key area | Process | Description of controls |
|---|---|---|---|
| | | 3. Service level management | **3.1 Service measurement and implementation:** An integrated Service Measurement Framework needs to be put in place that defines and collects the required metrics and raw data, and supports the reporting and interpretation of that data. IT services are assessed for quality reviews, benchmarking it against formal established service standards and reporting on where improvements are possible or needed and implemented as such.<br><br>**3.2 Service Reporting:**<br>IT needs to build an actionable approach to reporting, i.e. what happened, what IT did, how IT will ensure it doesn't impact the business again and how IT are working to improve service delivery in general as well as reporting on the return on IT investments made. |
| | | 4. Other life-cycle stages applicable in CSI | Change, release and deployment, availability, capacity, knowledge, problem, organisational and service continuity management principles. |

## Appendix 3: ISO 27002 standard and controls

| Nr | Key area | Process | Description of ISO 27002 controls |
|---|---|---|---|
| **1.** | **Information security policy and its organisational management** | 1.1 Internal organisational structure | Management framework for information security should be implemented, documenting senior management's commitment, the company's direction as well as authorisation and accountability policies. The roles and responsibilities such as detailed job descriptions and IT security responsibilities are defined. Authorise and evaluate procedures for new and modified information processing systems including authorise IT facilities and independently review the information security systems. The information security concerns should be communicated throughout the organisation. |
| | | 1.2 External parties | Risk assessments, contractual and confidentiality agreements should be in place with third-party suppliers, users and the relevant authorities. |
| **2.** | **Asset management** | 2.1 Responsibility for assets | Perform and maintain accurate inventory counts of information assets such as IT hardware, software, data, system documentation, storage media and supporting assets such as UPS's and ICT services. The assets' location and ownership should also be recorded and its acceptable uses identified. |
| | | 2.2 Information classification | Classify and label information according to its need for security protection including managing the introduction, transfer, removal and disposal of all assets. |

| Nr | Key area | Process | Description of ISO 27002 controls |
|---|---|---|---|
| **3.** | **Human resources security** | 3.1 Prior, during and termination of employment | Employ the appropriate staff through pre-employment screenings, adequate job descriptions, employment terms and conditions, educate and train employees on security procedures as well as implement formal disciplinary processes to deal with security breaches. Corporate assets should be returned and users' access rights removed on termination. |
| **4**. | **Physical and environmental security** | 4.1 Secure areas | Implement layers of physical controls to protect sensitive IT facilities from unauthorised access including implementing physical access controls and asset transfer controls. |
| | | 4.2 Equipment security | Critical IT equipment and cabling components should physically be protected against environmental hazards such as fire, floods and theft both on-and off-site. |
| **5.** | **Communications and operations management** | 5.1 Operational procedures & responsibilities | Document IT operating responsibilities. Configuration and changes to IT facilities and systems should be controlled as well as controlling adequate segregation of duties between relevant staff such as segregation between the development and operational system's staff. |
| | | 5.2 Third-party service delivery management | Third-party service delivery matters should be controlled through the appropriate contractual agreements and security clauses. |
| | | 5.3 System planning and acceptance | Covers IT capacity planning and the acceptance of production processes. |

| Nr | Key area | Process | Description of ISO 27002 controls |
|---|---|---|---|
| | | 5.4 Protection against malicious and mobile code | Need for anti-malware controls and security controls for mobile code associated with middleware services. |
| | | 5.5 Back-up process | Covers routine back-ups and restoration procedures. |
| | | 5.6 Network security management | Covers matters w.r.t network security management, -monitoring and related controls, including security w.r.t private networks and firewalls. |
| | | 5.7 Media handling | Implement controls w.r.t. protecting documents and computer media containing data and system information. The disposal of backup media, documents and test data should be logged and controlled, including procedures relating to the secure handling, transporting and storing of backup media and system documentation. |
| | | 5.8 Exchange of information | The exchange of information between organisations should be controlled through policies, procedures and agreements and comply with the applicable legislation standards. Secure procedures relating to protecting information and physical media in transit including electronic messaging such as email, electronic data interchange (EDI) and business information systems, should be in place. |

| Nr | Key area | Process | Description of ISO 27002 controls |
|---|---|---|---|
| | | 5.9 Electronic commerce services | The security implications of e-Commerce (online transaction systems) should be evaluated and suitable controls implemented. The integrity and availability of information published online should also be protected. |
| | | 5.10 Monitoring | Covers logging of security events, audit trails and system alerts, in order to detect the unauthorised use of systems and information. |
| **6.** | **Access controls** | 6.1 Business requirements for access controls | Control the access to information assets, including the setup of job related user and terminal access profiles. |
| | | 6.2 User access management | Allocation of users' specific access rights, including password controls should be regularly reviewed. |
| | | 6.3 User responsibilities | Users need to be aware of their responsibilities towards maintaining effective access controls eg: choosing strong password controls and maintaining its confidentiality. |
| | | 6.4 Network access controls | Network access should be controlled both from within and between organisations. Remote users,-equipment and -ports should be authenticated and securely controlled. Information services, users and systems should be segregated into separate logical network domains. Network connections and routine access paths should be controlled where necessary. |

| Nr | Key area | Process | Description of ISO 27002 controls |
|---|---|---|---|
| | | 6.5 Operating system access control | Operating systems should control utilities such as user authentication implementing unique user ID's, manage passwords, record use of privileges and system security alarms. |
| | | 6.6 Application and information access controls | Access to application systems should be controlled in terms of a defined access control policy. Certain sensitive applications may require dedicated (isolated) platforms and additional controls if run on shared platforms. |
| | | 6.7. Mobile computing and teleworking | Formal policies should be in place to secure the use of portable PC's, PDA's, cell-phones, secure teleworking and other forms of mobile and remote working stations, as well as defining its respective routing paths. |
| **7.** | **Information systems acquisition, development and maintenance** | 7.1 Security requirements of information systems | Automated and manual security control requirements should be analysed and identified during the stages of system development or the acquisition stage and incorporated into business cases. Purchased software should be risk assessed and formally tested for security related matters. |
| | | 7.2 Correct processing in application systems | Data input, processing and output validation controls and message authentication controls should mitigate integrity risks. |

| Nr | Key area | Process | Description of ISO 27002 controls |
|---|---|---|---|
| | | 7.3 Cryptographic controls | A cryptography policy should be in place, covering roles and responsibilities, digital signatures, non-repudiation and management of keys-and-digital certificates. |
| | | 7.4 Security of system files | Access to system files (both executable and source code) and test data should be controlled. |
| | | 7.5 Security in development and support processes | Application system managers should be responsible for controlling access to development project and support environments. Formal change control processes should be applied including technical reviews, supervisory and monitoring controls. |
| | | 7.6 Technical vulnerability management | Monitor technical vulnerabilities in systems and applications documenting the relevant security weaknesses and risk assessment results. |
| **8.** | **Information security incident management** | 8.1 Reporting information security incidents and weaknesses | Report incidents together with its corresponding response and escalation procedures. A central point of contact for all parties should be established as well as their own incident reporting responsibilities. |

| Nr | Key area | Process | Description of ISO 27002 controls |
|---|---|---|---|
| | | 8.2 Management of information security incidents and improvements | Responsibilities and procedures should be established to manage incidents consistently and effectively and implement continuous improvements. |
| **9**. | **Business continuity management** | | Strong interactions between the IT disaster recovery plan, business continuity management and contingency planning should be in place ranging from analysing, documenting and testing of these plans. |
| **10.** | **Compliance** | 10.1 Compliance with legal requirements | A company must comply with the applicable legislation such as copyright, data protection, protection of financial data and other vital data records, relevant legislation, intellectual property rights, data privacy and prevention of data misuse. |
| | | 10.2 Compliance with security policies, standards and technical compliance | Managers and system owners must ensure compliance with security policies and standards through regular testing security platforms. |
| | | 10.3 Information system's audit considerations | Audits should be carefully planned to minimise disruption to operational systems. Powerful audit tools and facilities should also be protected against unauthorised uses. |

## Appendix 4 – COBIT processes aligned with the business imperatives

| | Inno-vation | Afford-ability | Diverse products | Ease of use | Regul. Compl. | Mobility | Reliability | Pro-active manage-ment | Collaboration | Productivity | Customer service | Replication |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PO1 | X | X | X | X | X | X | X | X | X | X | X | X |
| PO2 | X | X | X | X | X | X | X | X | X | X | X | X |
| PO3 | X | X | X | X | X | X | X | X | X | X | X | X |
| PO4 | X | X | X | X | X | X | X | X | X | X | X | X |
| PO5 | X | X | X | | | | | X | | X | X | X |
| PO6 | X | X | X | X | X | X | X | X | X | X | X | X |
| PO7 | X | X | X | X | X | X | X | X | X | X | X | X |
| PO8 | X | X | X | X | X | X | X | X | X | X | X | X |
| PO9 | X | X | X | | X | X | X | X | X | X | X | X |
| PO10 | X | | X | | | | | | | | | X |
| AI1 | X | X | X | X | | X | X | X | X | X | X | X |
| AI2 | X | X | X | X | X | X | X | X | X | X | X | X |
| AI3 | X | X | X | X | X | X | X | X | X | X | | X |
| AI4 | X | X | X | X | X | X | X | X | X | X | X | X |
| AI5 | X | X | X | X | | X | X | | X | X | X | X |
| AI6 | X | X | X | X | X | X | X | X | | X | | X |
| AI7 | X | | X | | X | | X | X | | X | | X |
| DS1 | X | X | X | X | X | X | X | X | X | X | X | X |
| DS2 | X | X | X | X | | X | X | | X | X | X | X |
| DS3 | X | | X | | | | | | X | | X | |
| DS4 | | | | | X | X | X | X | X | X | X | X |
| DS5 | X | X | X | | X | X | X | X | X | X | X | X |
| DS6 | X | X | X | | | | | X | | X | | |
| DS7 | X | X | X | X | X | X | X | X | X | X | X | X |
| DS8 | X | X | X | X | X | X | X | X | X | X | X | X |
| DS9 | X | | X | X | X | X | X | X | X | | | X |
| DS10 | X | X | X | X | X | X | X | X | X | X | X | X |
| DS11 | X | X | X | X | X | X | X | X | X | X | X | X |
| DS12 | | X | X | X | X | X | X | X | X | X | | X |
| DS13 | X | X | X | X | X | X | X | X | X | X | X | X |
| ME1 | X | X | X | X | X | X | X | X | X | X | X | X |
| ME2 | X | X | X | X | X | X | X | X | X | X | X | X |
| ME3 | X | | | | X | X | X | X | X | | X | |
| ME4 | X | X | X | X | X | X | X | X | X | X | X | X |

## Appendix 5: Mapping between the COBIT control framework, ITIL control model and ISO 27002 standard's processes

| COBIT | COBIT process | COBIT controls | ITIL area and controls | ISO 27002 controls |
|---|---|---|---|---|
| PO1 | Define a strategic IT plan | • Determine business strategies and goals<br>• Implement business-IT alignment procedures<br>• perform accurate IT resource management activities | **Service strategy:**<br>1. Determine business service requirements and market share<br>2.1 – 2.3 Determine IT policies and strategies at organisational, operational and technological level<br>3. Financial management and Return on investments<br>4. Service portfolio management<br>5. Demand management<br><br>**Service design:**<br>1.1 Determine the business service requirements<br>1.3 Determine the service solutions and service portfolios<br><br>**CSI:**<br>3.1 Service measurement and implementation | Not applicable |
| PO2 | Define the information architecture | • Maintain IT architecture components to provide reliable information<br>• Ensures quality decision-making processes<br>• Data management: determine data ownership, classification and encryption activities<br>• Integrity management: policies ensuring data integrity in electronic format | **Service design:**<br>1.1 Design the business service management system<br>1.4 Design the IT architecture structures<br>9. Data and information management<br>12. Technological considerations | 2. Asset management (2.1 – 2.2)<br>5. Communications and operations management:<br>5.7 Media handling<br>5.8 Exchange of information<br>6. Access controls:<br>6.1 Business requirements for access controls |
| PO3 | Determine technological direction | • Design IT infrastructure plan including IT strategic direction, acquisition procedures, architecture standards | **Service strategy:**<br>2.2 – 2.3 Determine IT policies and strategies at operational and technological level<br><br>**Service design:**<br>1.4 Design the IT architecture structures<br>5. Capacity management | 1.Information security policies and its organisational management<br>5. Communications and operations management:<br>5.3 System planning and acceptance<br>5.8 Exchange of information<br>6. Access controls:<br>6.7 Mobile and teleworking computing<br>9. Business continuity management |

| COBIT | COBIT process | COBIT controls | ITIL area and controls | ISO 27002 controls |
|---|---|---|---|---|
| PO 4 | Define IT processes, organisation and relationships | • Define IT processes and functions via an IT process framework<br>• Develop IT organisational structure determining roles and responsibilities and committee setups | **Service strategy:**<br>2.1 – 2.3 Determine IT policies and strategies at organisational, operational and technological level<br><br>**Service design:**<br>1.4 Design the IT architecture structures<br>1.5 Design the IT processes<br>1.6 Design the measurement systems and criteria<br>2. Service level management<br>11. Organisational management<br>13. service design implementation<br><br>**Service transition:**<br>1. Service transition policies<br>3. Change management<br>7. Organisational support<br>8. Service validation, testing and implementation<br><br>**Service operations:**<br>1.Service operations policies<br>6. Organisational management<br>7.1 – 7.4 Problem management functional processes<br>8. Common service operational activities<br>8.3 Infrastructure management<br>9. Service operation's implementation<br><br>**CSI:**<br>1.CSI policies and procedures<br>2. 7 step improvement process<br>3.1 Service measurement | 1.Information security policies its organisational management of the policy (1.1 - 1.2)<br>2. Asset management:<br>2.1 Responsibility for assets<br>3. Human resource security management<br>(prior and during employment)<br>4. Physical and environmental security: (4.1 – 4.2)<br>5. Communications and operations management:<br>5.1 Operational procedures and responsibilities<br>5.6 Network security management<br>10. Compliance:<br>10.1- 10.2 Comply with legal requirements and security policies and standards |

| COBIT | COBIT process | COBIT controls | ITIL area and controls | ISO 27002 controls |
|---|---|---|---|---|
| PO5 | Manage IT investments | • Determine the effective and efficient use of IT resources<br>• Budget vs actual financial return on IT assets | **Service strategy:**<br>1. Determine business service requirements and market share<br>3. Financial management and Return on investments<br>4. Service portfolio management<br><br>**Service transition:**<br>6. Release and deployment management<br><br>**Service operation:**<br>8.4 Financial management for IT services (as operational activities) | 1.Information security policies and organisational management of the policy<br>8. Information security incident management:<br>8.1 Reporting information security incidents and weaknesses |
| PO6 | Communicate management aims and direction | • IT control framework policies are communicated to the company<br>• Communicate the direction, service objectives, IT risks. | **Service strategy:**<br>2.1 Determine IT policies and strategies at organisational level<br><br>**Service transition:**<br>1. Service transition policies<br><br>**Service operation:**<br>6. Organisational management | 1.Information security policies its organisational management<br>2. Asset management:<br>2.1 Responsibility for assets<br>3. Human resource security<br>4. Physical and environmental security: (4.1 – 4.2)<br>5. Communications and operations management:<br>5.7 Media handling<br>5.8 Exchange of information<br>5.9 Electronic commerce services<br>6. Access controls (6.1 – 6.7)<br>7. Information systems acquisition, development and maintenance management:<br>7.1 Security requirements of information systems<br>8. Information security incident management:<br>8.1 Reporting information security incidents and weaknesses<br>10. Compliance:<br>10.1-10.2 Compliance with legal requirements and with security policies, standards and technical compliance |

| COBIT | COBIT process | COBIT controls | ITIL area and controls | ISO 27002 controls |
|---|---|---|---|---|
| PO7 | Manage IT human resources | • Policies regarding the recruiting, training, promoting and terminating of IT staff | **Service design:**<br>11. Organisational management | 3. Human resource security |
| PO8 | Manage quality | • Implement quality management system<br>• Ensure IT delivers value to the company<br>• Continuously improve quality standards and services | **Service strategy:**<br>2.1-2.2 Determine IT policies and strategies at organisational and operational level<br>5. Demand management<br><br>**Service design:**<br>1. Service design aspects: 1.1 – 1.6 principles<br>2. Service level management<br>10. Application management<br>12. Technological considerations<br><br>**Service transition:**<br>1. Service transition policies<br>2. Service transition, planning and support<br>6. Release and deployment management<br>8.Service validation and testing and implementation<br><br>**CSI:**<br>1.CSI policies and procedures<br>2. The seven-step improvement process<br>3.1 Service measurement & implementation<br>3.2 Service reporting<br>4. Organisational management | 1.Information security policies and its organisational management<br>7. Information systems acquisition, development and maintenance |
| PO9 | Assess and manage IT risks | • Develop risk management policies<br>• Implement risk mitigation strategies | **Service strategy:**<br>6. Risk management<br><br>**Service design:**<br>8. IT service continuity management<br>13. Service deign implementation<br><br>**Service transition:**<br>9. Evaluation<br><br>**CSI:**<br>4. IT service continuity management | 1.Information security policies and its organisational management<br>8.Information security incident management:<br>8.1 reporting information security incidents and weaknesses<br>9. Business continuity management |

| COBIT | COBIT process | COBIT controls | ITIL area and controls | ISO 27002 controls |
|---|---|---|---|---|
| PO10 | Manage projects | • Develop IT project management policies<br>• Coordinate and allocate resources<br>• Determine list of deliverables<br>• User approval<br>• Formal test plan and post – implementation reviews | **Service design:**<br>1.1 Determine the business service requirements<br>1.2 Determine the design and acquisition standards<br><br>**Service transition:**<br>1. Service transition policies<br>2. Service transition, planning and support | Not applicable |
| AI1 | Identify automated solutions | • Analyse business needs before new application is required/ developed<br>• Determine the technology, risks and cost vs benefit requirements of application | **Service strategy:**<br>2.2 -2.3 Determine IT policies and strategies at operational and technological level<br><br>**Service design:**<br>1. Service design aspects: 1.1 – 1.8 principles<br>5. Capacity management<br>8. IT service continuity management<br>12. Technological considerations<br><br>**Service transition:**<br>1. Service transition policies<br><br>**Service operation:**<br>7.4 IT operations management | 1.Information security policies and its organisational management<br>3. Human resource security (during employment)<br>5. Communications and operations management:<br>5.3 Systems planning and acceptance<br>6. Access controls:<br>6.6 Application and information access controls<br>7. Information systems acquisition, development and maintenance:<br>7.1 Security requirements of information systems |

| COBIT | COBIT process | COBIT controls | ITIL area and controls | ISO 27002 controls |
|---|---|---|---|---|
| AI2 | Acquire and maintain application software | • Implement design policies for application<br>• Develop relevant security and configuration requirements of application | **Service strategy:**<br>2.3 Determine IT policies and strategies at technological level<br><br>**Service design:**<br>1.3 Design the service solutions and service portfolios<br>1.4 Design the IT architecture structures<br>2. Service level management<br>10. Application management<br><br>**Service transition:**<br>1. Service transition policies<br><br>**Service operation:**<br>7. Problem management | 1.Information security policies and its organisational management<br>2. Asset management:<br>2.2 information classification<br>5. Communications and operations management:<br>5.3 Systems planning and acceptance<br>5.10 Monitoring<br>Access controls:<br>6.6 Application and information access controls<br>7. Information systems acquisition, development and maintenance (7.1 – 7.5)<br>8.Information security incident management<br>10. Compliance:<br>10.3 information systems' audit considerations |
| AI 3 | Acquire and maintain technology infrastructures | • Implement formal processes to acquire, implement and upgrade technical infrastructures<br>• Implement internal controls<br>• Develop security, configuration and maintenance standards<br>• Ensure data integrity and availability<br>• Perform integration tests on implemented applications | **Service design:**<br>1.4 Design the IT architecture structures<br>7. IT security management<br><br>**Service transition:**<br>6. Release and deployment management<br>8. Service validation , testing and implementation<br><br>**Service operation:**<br>8.3 Infrastructure management | 4. Physical and environmental security (4.1 – 4.2)<br>5. Communications and operations management:<br>5.1 Operational procedures and responsibilities<br>7. information systems acquisition, development and maintenance:<br>7.1 Security requirements<br>7.4 Security of system files<br>7.5 Security in development and support process<br>7.6 Technical vulnerability management |

| COBIT | COBIT process | COBIT controls | ITIL area and controls | ISO 27002 controls |
|---|---|---|---|---|
| AI 4 | Enable operation and use | • Communicate new system knowledge via documentation and manuals<br>• Train end-users and IT staff | **Service design:**<br>1.3 Design the service solutions and service portfolios<br><br>**Service transition:**<br>1. Service transition policies<br>6. Release and deployment management<br>7. Knowledge management<br><br>**Service operations:**<br>6. Organisational management<br>7. Problem management<br>8.4 Knowledge management (as operational activities)<br><br>**CSI:**<br>5. Knowledge management | 5. Communications and operations management:<br>5.1 Operational procedures and responsibilities<br>5.3 System planning and acceptance<br>5.7 Media handling<br>8. Information security incident management<br>8.2 Management of information security incident and improvements |
| AI 5 | Procure IT resources | • Develop a formal procurement process to procure the correct people, hardware, software and supplier services. | **Service design:**<br>1.7 Evaluate alternative solutions and procure the correct solution<br>2. Service level management<br>4. Supplier management | 1.Information security policies and its organisational management<br>5. Communications and operations management:<br>5.8 Exchange of information<br>7. Information systems acquisition, development and maintenance:<br>7.5 Security in development and support processes |

| COBIT | COBIT process | COBIT controls | ITIL area and controls | ISO 27002 controls |
|---|---|---|---|---|
| AI 6 | Manage change | • Changes to procedures, processes and systems should be recorded, evaluated and authorised. | **Service design:**<br>1.7 Evaluate alternative solutions and procure the correct solution<br><br>**Service transition:**<br>1. Service transition policies<br>2. Service transition, planning and support<br>3. Change management<br>4. Organisational support<br>6. Release and deployment management<br>9. Evaluation<br><br>**Service operation:**<br>5. Request management<br>8.4 Change management (as operational activities)<br><br>**CSI:**<br>4.Change, release and deployment management | 5. Communications and operations management:<br>5.1 Operational procedures and responsibilities<br>6. Access controls:<br>6.5 Operating system access controls<br>7. Information systems acquisition, development and maintenance:<br>7.5 Security development and support processes<br>7.6 Technical vulnerability management |
| AI 7 | Install and accredit solutions and changes | • Perform detailed testing on new systems<br>• Perform post-implementation reviews | **Service transition:**<br>1. Service transition policies<br>2. Service transition, planning and support<br>6. Release and deployment management<br>8. Service validation, testing and implementation<br>9. Evaluation<br><br>**Service operations:**<br>5. Request management<br>8.4 Release and deployment management (as operational activities)<br><br>**CSI:**<br>4. Change, release and deployment management | 1.Information security policies and its organisational management<br>3. Human resource security (during employment)<br>5. Communications and operations management:<br>5.1 operational procedures and responsibilities<br>5.3 System planning and acceptance<br>7. Information systems acquisition, development and maintenance<br>7.4 Security of system files<br>7.5 security in development and support processes |

| COBIT | COBIT process | COBIT controls | ITIL area and controls | ISO 27002 controls |
|---|---|---|---|---|
| DS1 | Define and manage service levels | • Determine the extent of IT services and levels to be delivered to the company. | **Service strategy:**<br>1. Determine business service requirements and market share<br>2.1 – 2.3 Determine IT policies and strategies at organisational, operational and technological level<br>4. Service portfolio management<br>5. Demand management<br><br>**Service design:**<br>1.1 Determine the business service requirements<br>1.2 Determine the development and acquisition standards<br>1.3 Determine the service solutions and service portfolios<br>2. Service level management<br>3. Service catalogue Management<br>5. Capacity management<br>9. Data and information management<br>13. Service design implementation<br><br>**Service operations:**<br>6. Organisational management<br><br>**CSI:**<br>3. Service level management (3.1 – 3.2) | 5. Communications and operations management:<br>5.2 Third-party service delivery management |

| COBIT | COBIT process | COBIT controls | ITIL area and controls | ISO 27002 controls |
|---|---|---|---|---|
| DS 2 | Manage third-party services | • Define third parties' roles, responsibilities and services rendered<br>• Review compliance with agreements and effectiveness of services delivered | **Service strategy:**<br>2.1 - 2.2 Determine IT policies and strategies at organisational and operational level<br><br>**Service design:**<br>4. Supplier management | 1.Information security policies and its organisational management<br>3. Human resource security (prior employment)<br>5. Communications and operations management:<br>5.2 Third-party service delivery management<br>5.8 exchange of information<br>7. Information systems acquisition, development and maintenance<br>7.4 Security of system files<br>7.5 security in development and support processes<br>10. Compliance:<br>10.1 Compliance with legal requirements |
| DS3 | Manage performance and capacity | • Review on regular basis the current abilities of IT resources<br>• Determine future business needs i.to.IT services required. | **Service design:**<br>5. Capacity management<br>6. Availability management<br><br>**Service operations**<br>2. Event management<br>8.1 Monitoring and control (performance monitoring)<br>8.3 infrastructure management<br>8.4 Capacity management (as operational activities)<br>8.4 Availability management (as operational activities)<br><br>**CSI:**<br>3.1 Service measurement and implementation<br>4. Availability and Capacity management | 5. Communications and operations management:<br>5.3 System planning and acceptance |
| DS4 | Ensure continuous services | • Provide continued IT services by:<br>• Develop, maintain and test IT continuity plans,<br>• Perform off site backups and periodic continuity training | **Service design:**<br>6. Availability management<br>8. IT service continuity Management<br><br>**Service operations:**<br>8.3 Infrastructure management<br>8.4 IT service continuity management<br>**CSI:**<br>4.IT service continuity management | 1.Information security policies and its organisational management<br>5. Communications and operations management:<br>5.5 Back up processes<br>9. Business continuity management |

| COBIT | COBIT process | COBIT controls | ITIL area and controls | ISO 27002 controls |
|---|---|---|---|---|
| DS5 | Ensure systems security | • Implement security systems that will ensure information's integrity and protection of IT assets. | **Service design:**<br>7. IT security management<br><br>**Service operations:**<br>3. Access management<br>8.3 infrastructure management | 1.Information security policies and its organisational management<br>3. Human resource security<br>4. Physical and environmental security (4.1 + 4.2)<br>5. Communications and operations management:<br>5.1 Operational procedures and responsibilities<br>5.4 Protection against malicious and mobile code<br>5.6 Network security management<br>5.7 Media handling<br>5.8 Exchange of information<br>5.9 Electronic commerce services<br>5.10 Monitoring<br>6. Access controls:<br>6.1 Business requirements for access controls<br>6.2 User access management<br>6.3 User responsibilities<br>6.4 Network access controls<br>6.5 Operating system access controls<br>6.6 Application and information access controls<br>6.7 Mobile computing and teleworking<br>7. Information systems acquisition, development and maintenance<br>7.2 correct processing in application systems<br>7.3 Cryptographic controls<br>7.4 security of system files<br>7.6 Technical vulnerability management<br>8. Information security incident management:<br>8.1 – 8.2 Reporting and management of security incidents and weaknesses<br>10. Compliance:<br>10.1 Compliance with legal requirements<br>10.2 Compliance with security policies, standards and technical compliance<br>10.3 Information system's audit considerations |

| COBIT | COBIT process | COBIT controls | ITIL area and controls | ISO 27002 controls |
|---|---|---|---|---|
| DS6 | Identify and allocate assets | • Measure, report and link IT costs to a specific user and business process. | **Service strategy:**<br>2.2 Determine IT policies and strategies at operational level.<br>3. Financial management and return on investment<br><br>**Service design:**<br>3. Service catalogue Management<br><br>**Service operations:**<br>8.4 Financial management for IT services (as operational activities) | Not applicable |
| DS7 | Educate and train users | • Train all IT users | **Service operations:**<br>8.3 Infrastructure management | 3. Human resource security (during employment) |
| DS8 | Manage service desk and incidents | • Analyse, respond and resolve in a timely manner, IT users' queries and problems. | **Service operations:**<br>2. Event management<br>4. Incident management<br>5. Request management<br>7.1 Desktop support | 8. Information security incident management:<br>8.1 – 8.2 Reporting and management of security incidents and weaknesses<br>9. Business continuity management |
| DS9 | Manage configurations | • Ensure hardware and software configuration setups are accurately determined. | **Service strategy:**<br>2.3 Determine IT policies and strategies at technological level<br><br>**Service transition:**<br>2.Service transition, planning and support<br>4. Service asset and configuration management<br><br>**Service operations:**<br>8.3 Infrastructure management<br>8.4 Configuration management (as operational activities) | 2. Asset management: (2.1 – 2.2)<br>5. Communications and operations management:<br>5.7 Media handling<br>*6.* Access control:<br>6.4 Network access controls<br>7. Information systems acquisition, development and maintenance<br>7.4 Security of system files<br>7.5 Security in development and support processes<br>7.6 Technical vulnerability management<br>10 .Compliance<br>10.1 Compliance with legal requirements |
| DS10 | Manage problems | • Identify, classify, analyse and resolve IT problems raised in order to create an optimum available system and improve customer satisfaction levels. | **Service operations:**<br>7. Problem management<br>**CSI:**<br>4. Problem management | 8. Information security incident management:<br>8.1 Reporting information security incidents and weaknesses |

| COBIT | COBIT process | COBIT controls | ITIL area and controls | ISO 27002 controls |
|---|---|---|---|---|
| DS11 | Manage data | • Management of data by managing the media library, data recovery, disposal of media. This will enhance the quality, timeliness and availability of data. | **Service design:**<br>9. Data and information management<br><br>**Service operations:**<br>8.3 Infrastructure management | 4. Physical and environmental security:<br>4.2 Equipment security<br>5. Communications and operations management:<br>5.5 Back –up processes<br>5.7 Media handling<br>5.8 Exchange of information<br>7. Information systems acquisition, development and maintenance:<br>7.4 Security of system files<br>10. Compliance:<br>10.1 Compliance with legal requirements |
| DS 12 | Manage physical environment | • Secure IT resources by physically controlling the environment and access to the resources. | **Service operations:**<br>8.3 Infrastructure management | 1.Information security policies and its organisational management<br>4. Physical and environmental security:<br>4.1 Secure areas<br>4.2 Equipment security |
| DS13 | Manage operations | • Ensure the complete and accurate processing of data by monitoring the IT infrastructures and maintaining the hardware components. | **Service design:**<br>5. Capacity management<br><br>**Service operations:**<br>2. Event management<br>6. Organisational management<br>7.4 IT operations management<br>8.1 Monitoring and control<br>8.2 IT operations<br>8.3 Infrastructure management | 4. Physical and environmental security:<br>4.2 Equipment security<br>5. Communications and operations management:<br>5.1 Operational procedures and responsibilities<br>5.7 Media handling |

| COBIT | COBIT process | COBIT controls | ITIL area and controls | ISO 27002 controls |
|---|---|---|---|---|
| ME1 | Monitor and evaluate IT performance | • Monitor and measure the effectiveness of the IT department's performances and service levels. | **Service design:**<br>2. Service level management<br>13. Service design implementation<br><br>**Service transition:**<br>8. Service validation, testing and implementation<br><br>**Service operations:**<br>6. Organisational management<br><br>**CSI:**<br>1. CSI policies and procedures<br>2 (a-g). The seven-step improvement process<br>3. Service level management (3.1 – 3.2) | 5. Communications and operations management:<br>5.10 Monitoring |
| ME2 | Monitor and evaluate internal control | • Establish an internal IT control framework which will identify and rectify control errors, which will in turn ensure an effective IT operations system and complying with laws and regulations. | Not applicable | 1.Information security policies and organisational management of the policy<br>5. Communications and operations management:<br>5.2 Third-party service delivery management<br>5.10 Monitoring<br>10. Compliance:<br>10.2 Compliance with security policies, standards and technical compliance<br>10.3 Information systems' audit considerations |
| ME3 | Ensure compliance with external requirements | • Implement a review programme which will ensure the company is complying with laws and regulations, as well as contractual agreements. | Not applicable | 1.Information security policies and its organisational management<br>10. Compliance:<br>10.1 Compliance with legal requirements |

| COBIT | COBIT process | COBIT controls | ITIL area and controls | ISO 27002 controls |
|---|---|---|---|---|
| ME4 | Provide IT governance | • Implement an effective governmental framework which will define organisational structures, roles and responsibilities, business – IT alignment processes and allocating leadership responsibilities. | **Service strategy:**<br>1. Determine business service requirements and market share<br>2.2 Determine IT policies and strategies at operational level.<br>6. Risk management<br><br>**Service design:**<br>1.1 The business' service requirements and business service management systems<br>1.6 The measurement systems and criteria<br><br>**CSI:**<br>1. CSI policies and procedures<br>3.1 Service measurement and implementation | 1.Information security policies and its organisational management<br>5. Communications and operations:<br>5.10 Monitoring |

## Appendix 6: Align COBIT processes to the international IT governance key areas and King III's IT governance principles

| | | | International IT governance key control areas | | | | |
|---|---|---|---|---|---|---|---|
| **COBIT** | **COBIT process description** | **King III principles (as per Table 1)** | **Strategic alignment** | **Value delivery** | **Risk management** | **Resource management** | **Performance measurement** |
| PO1 | Derive a strategic IT plan | 5.1;5.2;5.6 | × | | | | |
| PO2 | Define the information architecture | 5.1-5.4; 5.6 | × | | | × | |
| PO3 | Determine the technological direction | 5.3;5.4;5.6 | | | | × | |
| PO4 | Define IT processes, organisation & relationships | 5.3-5.7 | | | × | × | |
| PO5 | Manage IT investments | 5.1;5.4 | | × | | | |
| PO6 | Communicate management aims and direction | 5.1-5.3;5.5-5.7 | × | | × | | |
| PO7 | Manage IT human resources | 5.1-5.4; 5.6 | × | | | × | |
| PO8 | Manage quality | 5.1;5.2;5.4;5.6;5.7 | × | | | | × |
| PO9 | Assess and manage IT risks | 5.1-5.3;5.5-5.7 | × | | × | | |
| PO10 | Manage projects | 5.1;5.2;5.6 | × | | | | |
| AI1 | Identify automated solutions | 5.1;5.2;5.4;5.6 | × | × | | | |
| AI2 | Acquire and maintain applications | 5.1;5.2;5.4;5.6 | × | × | | | |
| AI3 | Acquire and maintain technology infrastructure | 5.3;5.4;5.6 | | | | × | |
| AI4 | Enable operation and use | 5.1;5.4 | | × | | | |
| AI5 | Procure IT resources | 5.3;5.4;5.6 | | | | × | |
| AI6 | Manage Change | 5.1;5.4 | | × | | | |
| AI7 | Install and accredit solutions and changes | 5.1;5.4 | | × | | | |
| DS1 | Define and manage service levels | 5.1-5.4; 5.6;5.7 | × | × | | × | × |
| DS2 | Manage third-party services | 5.1;5.3;5.4;5.5-5.7 | | × | × | | |
| DS3 | Manage performance and capacity | 5.3;5.4;5.6 | | | | × | |

| | | | International IT governance key control areas | | | | |
|---|---|---|---|---|---|---|---|
| **COBIT** | **COBIT process description** | **King III principles (as per Table 1)** | **Strategic alignment** | **Value delivery** | **Risk management** | **Resource management** | **Performance measurement** |
| DS4 | Ensure continuous services | 5.1;5.3-5.7 | | × | × | | |
| DS5 | Ensure system security | 5.3;5.5-5.7 | | | × | | |
| DS6 | Identify and allocate assets | 5.3;5.4;5.6 | | | | × | |
| DS7 | Educate and train users | 5.1;5.4 | | × | | | |
| DS8 | Manage service desk and incidents | 5.1;5.4 | | × | | | |
| DS9 | Manage configurations | 5.1; 5.3;5.4;5.6 | | × | | × | |
| DS10 | Manage problems | 5.1;5.4 | | × | | | |
| DS11 | Manage data | 5.1;5.4 | | × | | | |
| DS12 | Manage physical environment | 5.3;5.5-5.7 | | | × | | |
| DS13 | Manage operations | 5.3;5.4;5.6 | | | | × | |
| ME1 | Monitor and evaluate IT performances | 5.1-5.2;5.4;5.6-5.7 | | | | | × |
| ME2 | Monitor and evaluate internal control | 5.1;5.3;5.4;5.5-5.7 | | × | × | | |
| ME3 | Ensure compliance with external requirements | 5.1-5.3;5.5-5.7 | × | | × | | |
| ME4 | Provide IT governance | 5.1 – 5.7 | × | × | × | × | × |

## Appendix 7: Align business imperatives to the international IT governance key control areas and King III's IT governance principles

| | | | International IT governance key control areas | | | | |
|---|---|---|---|---|---|---|---|
| | **Business imperative** | **King III principles (as per Table 1)** | **Strategic Alignment** | **Value delivery** | **Risk management** | **Resource management** | **Performance measurement** |
| 1. | Innovation | 5.1 – 5.7 | × | × | × | × | × |
| 2. | Affordability | 5.1 – 5.7 | × | × | × | × | × |
| 3. | Diverse products | 5.1 – 5.7 | × | × | × | × | × |
| 4. | Ease of use | 5.1 – 5.7 | × | × | × | × | × |
| 5. | Regulatory compliance | 5.1 – 5.7 | × | × | × | × | × |
| 6. | Mobility | 5.1 – 5.7 | × | × | × | × | × |
| 7. | Reliability | 5.1 – 5.7 | × | × | × | × | × |
| 8. | Pro-active management | 5.1 – 5.7 | × | × | × | × | × |
| 9. | Collaboration | 5.1 – 5.7 | × | × | × | × | × |
| 10. | Productivity | 5.1 – 5.7 | × | × | × | × | × |
| 11. | Customer service | 5.1 – 5.7 | × | × | × | × | × |
| 12. | Replication | 5.1 – 5.7 | × | × | × | × | × |