# FORMULATING AN IT GOVERNANCE FRAMEWORK

**A thesis submitted in fulfilment of the requirements for the degree of**

**MASTER OF COMMERCE**

**of**

**RHODES UNIVERSITY**

**by**

**PIETER ROOS**

**November 2014**

## Abstract

Modern organisations make substantial investments in Information Technology (IT). Corporate governance practices can no longer ignore the importance of effectively governing IT. Consequently, the third King Report on Corporate Governance (King III) makes specific provision for IT governance, which is implemented through the establishment of an IT governance framework. The purpose of this research is to develop a generic IT governance framework, suitable to any large South African organisation in the public or private sector.

The literature considered for this research confirmed the extent of standards and practices available in support of IT governance, together with the roles and structures required to implement them. These included well-known publications such as COBIT, Prince2, ITIL and ISO/IEC27000. Based on the literature review, a theoretical Processes, Enablers and Structures (PES) IT Governance Framework was formulated. The framework was further explored by means of a survey of and structured interview with ten Chief Information Officers (CIOs) of South African organisations with a turnover in excess of R1bn per annum.

The final PES IT Governance Framework comprises three dimensions, each of which contains a set of constituent components:

- Processes: Strategic Alignment, Value Delivery, Resource Management, Risk Management and Performance Measurement.
- Enablers: IT Sub Processes, Supporting Documentation, IT Control Framework, Technology Architecture, Desirable Practice, IT Portfolio Management and Regulation.
- Structures: The Board, Office of the CIO, IT Steering Committee, Technology Architecture Forum, IT Programme Management Office and Information Security Organisation.

As the number of regulatory requirements and associated compliance pressures grow, the importance of an effective IT governance framework also becomes more prominent. The PES IT Governance Framework offers a uniquely practical approach to addressing IT governance principles that are often regarded as abstract.

The final PES IT Governance Framework provides clear guidance on how organisations could implement an IT governance framework, which addresses the strategic alignment of IT to business, value delivery by IT investments, IT risk management, IT resource management and IT performance measurement.

# Acknowledgements

## Interviewees

The ten Chief Information Officers who agreed to participate in this research

## Proofing Early Drafts

Altus Viljoen

# TABLE OF CONTENTS

## List of Tables

# List of Figures

## Acronyms

BMIS: The Business Model for Information Security - a complementary framework to COBIT, published by the IT Governance Institute to promote business-focused information security practices.

CIO: Chief Information Officer.

CMMI: The Capability Maturity Model Integration (CMMI) - a process improvement programme administered by Carnegie Mellon University, mainly applied to software development, but also utilised by COBIT up to COBIT 4.1.

COBIT: A framework for the governance of enterprise IT (COBIT 5). Up to COBIT 4.1, this was mainly a set of control objectives, published as the Control Objectives for Information and Related Technology. COBIT 5 retained the COBIT brand but no longer presented itself as a set of control objectives. Instead, it presented as a more extensive governance framework for enterprise IT.

COSO: The Committee of Sponsoring Organizations of the Treadway Commission - a thought leadership initiative by five private sector organisations, providing guidance on enterprise risk management, the control environment and fraud deterrence.

CTO: Chief Technology Officer.

EPMO: Enterprise Programme Management Office. See definition of PMO below. An enterprise-wide instance of the PMO.

ISO: The International Standards Organisation.

ISO/IEC20000: The International Standards Organisation's standard for information technology service management. Also see ITIL.

ISO/IEC27001: The International Standards Organisation's standards for information security management systems and related techniques. Preceded by British Standard BS7799 and the related ISO/IEC17799 standards.

ISO/IEC38500: The International Standards Organisation's standard for IT governance.

IT: Information Technology.

ITGI: The IT Governance Institute.

ISACA: The Information Systems Audit and Control Association.

ITIL: A collection of best practices for information technology service management, dealing with the service lifecycle from service strategy through to service operation. The original publications were grouped into the Information Technology Infrastructure Library which, like COBIT, became a strong brand and is still in use today, but spans much wider than infrastructure.

King III: The third King Report ("King III") on Corporate Governance to which all companies on the Johannesburg Securities Exchange must conform. Chapter Five of King III sets out the IT governance requirements for effective corporate governance.

KPI: Key Performance Indicator – measurement used to evaluate the success of an activity.

PES: The Processes, Enablers and Structures IT Governance Framework, proposed by the research for this dissertation.

PMBOK: Project Management Book of Knowledge – a publication by the Project Management Institute, presenting standard terminology and guidelines for project management.

PMI: The Project Management Institute – a United States of America professional organisation for advancing project management.

PMO: The Programme Management Office – a support function that sets the standards for portfolio, programme and project management, monitors compliance with these standards, facilitates the resourcing of projects, and reports on portfolio, programme and project management activities.

Prince2: Projects in controlled environments 2 – a project management method developed by the Office of Govenment Commerce (OGC) in the United Kingdom.

RiskIT: A complementary framework to COBIT, published by the IT Governance Institute to promote IT risk management practices.

ROI: Return On Investment – a metric used to evaluate the financial and non-financial gains as a result of an investment.

TOGAF: The Open Group Architecture Framework – an architecture framework developed by the Open Group Architecture Forum, up to release 8. At the time this dissertation was written, Capgemini was working on finalising release 9. The release referenced by this dissertation is the 9th, draft 4.

ValIT: A complementary framework to COBIT, also published by the IT Governance Institute, which provides structure to the measurement, monitoring and optimal realisation of business value from IT investment.

# Chapter One: Introduction

## 1.1 Introduction

A report by Forrester Research, Inc. (2007:8) concludes that the success of Chief Information Officers (CIOs) is at risk in the absence of a "good" Information Technology (IT) Governance Risk and Control (GRC) programme (Forrester, 2007:8). The IT Governance Institute (ITGI) supports this sentiment, claiming that effective IT governance supports alignment of IT and business goals, IT investment value optimisation and effective IT risk management (IT Governance Institute[a], 2006:2). Developments in enterprise governance and control, such as the proclamation of the Sarbanes-Oxley Act of 2002 in the United States of America (USA), have further focussed the attention on IT governance and internal control, leading to the publication of guidelines dealing specifically with IT controls (IT Governance Institute[b], 2006:12). Unfortunately, this has not translated into a common, global view of what an IT governance framework should be.

In a world where IT has an acronym for every challenge presented, it has become increasingly difficult to position best practices, methodologies and frameworks. For example, what works well for project management does not address the needs of IT operations. One tool does not fit all sizes (Brown, Grant, 2005:703). An IT governance framework is useful both in architecting an effective, modern IT function and in supporting compliance with the requirements of legislators, quality standards and business policies.

Following the "dot bomb era" after 2000, IT has had to work hard to re-establish credibility, only to now find itself once again competing for resources in a world that is facing increasing economic challenge. Perceptions that IT is not governed in line with organisational objectives or that it is acting wastefully cannot be curbed unless formal, demonstrable IT governance is practised. IT governance is an abstract topic that requires more than definitions and theories. The basis of the framework that this dissertation proposes is a model supported by best practices covering all aspects of IT, and lending it a more tangible character that is easy to explain and to translate into implementation plans.

## 1.2 Research Context

### 1.2.1 No Universally Appropriate Contemporary Framework

With the proliferation of press articles on the topic, corporate management now realise the importance of IT governance and are searching for appropriate, contemporary governance frameworks for their organisations (Brown, Grant, 2005:708). In recent years, an increased emphasis on corporate governance has also seen heightened responsibilities of senior management to formalise and improve the effectiveness of IT governance (Hamaker, 2005:242). In large organisations, IT fulfils a significant role as enabler of business transactions and integrating information exchange across organisational boundaries.

In a world where technologists have always had a tool handy for any eventuality, the realisation that governance cannot be equated with "tool" has not been a pleasant one (Gartner, 2008:1). With an abundance of tools and frameworks, it has become difficult to construct a single IT governance framework that could be implemented effectively and sustainably in any environment (De Haes, 2008:1). According to Brown and Grant (2005:703), "researchers are unanimous that a universal best IT governance structure does not exist." The inability to find a single IT governance framework that is effective across many organisations is true despite the positive developments for IT governance brought to many global companies by the introduction of the Sarbanes-Oxley Act, which focused on the control framework, a portion of the IT governance definition used in this dissertation.

### 1.2.2 No Single, Cohesive View of IT Governance

According to the National Computing Centre (NCC), "a shared, cohesive view of IT Governance is needed across the enterprise based on a common language" (National Computing Centre, 2005:7). In practice, however, IT governance initiatives often end up being scattered across the organisation and prove difficult to synchronise or consolidate (Forrester Research, 2007:6). In recent years, IT governance has continued to evolve. Many articles have been written about aspects of IT governance, but little definitive work has been done to consolidate these aspects (Hamaker, 2004:1). The single, consistent view of IT governance across intra and extra-organisational boundaries continues to elude IT governance practitioners.

### 1.2.3 Lack of Understanding of Concept of IT Governance Framework

The IT Governance Institute's Global Status Report on the Governance of Enterprise IT – 2011, showed that the IT Infrastructure Library (ITIL) was still the most widely adopted IT governance framework (28%), as also indicated by the 2008 report. This indicates a focus by most organisations on IT service management only, rather than adopting a more comprehensive framework governing the entire IT function. The report further highlights that only 12.9% of the organisations included in the survey have adopted COBIT, with an equal number of organisations having opted for an internally developed framework. This indicates a lack of understanding by most organisations of IT service management vs. that of a comprehensive IT governance framework.

### 1.2.4 Summary

In summary, the following problems exist internationally with regard to the concept of a universally accepted IT governance framework: there are arguments towards the fact that no universal framework exists that is appropriate for most large organisations; no single, cohesive view of IT governance exists in most organisations; and there is an inadequate understanding of the concept of an IT governance framework in most global organisations. Based on the above and the absence of publications to the contrary, there appears to be no single generic IT governance framework that would enable organisations to formulate their own IT governance frameworks.

## 1.3 Research Objectives

The objectives of this research are to:

(i) Identify appropriate, generic best practices supporting IT governance;

(ii) Formulate a generic IT governance framework that incorporates all the identified IT governance best practices for use in any IT environment; and

(iii) Explore the feasibility of the generic IT governance framework through interviewing Chief Information Officers of large South African companies and recommending a generic model they could use to consolidate their IT governance structures and initiatives for improved effectiveness and sustainability.

## 1.4 Research Methodology

### 1.4.1 Overarching Methodology

The research methodology followed will be qualitative in nature, using an interpretive approach. Qualitative data sources include interviews, questionnaires, observation, documents and texts, combined with the researcher's impressions and reactions (Myers, 1997:242). The interpretive approach relies on the meanings people assign to phenomena, in order to understand such phenomena (Myers, 1997:243). The qualitative method employed is grounded theory (Myers, 1997:246), which follows an inductive approach to develop theory grounded in data that is systematically gathered and analysed. This allows the researcher to create a theroretic account of the general features of the research topic, whilst grounding the account in empirical data.

### 1.4.2 Descriptive Component – Research Steps

(i) Summarise relevant components of sources contributing to the research, according to the aspects that need to be covered to populate the IT governance framework.

(ii) Using the publications of the IT Governance Institute as a basis, formulate the generic IT governance framework.

(iii) Using a combination of best practices, customise the framework, which will be formulated to cover the IT Governance Institute's five major processes (the "what" dimension), generic roles and structures (the "who" dimension) and the enabling components or contents (the "how" dimension).

### 1.4.3 Empirical Work – Application

The research targets the offices of the CIO in ten large local organisations with a turnover in excess of R1bn per annum, to compare their governance structures to the proposed model as a test of the completeness of the model and the ability of the model to expose shortcomings in the IT governance structures of these organisations. The accessibility of the CIOs or their representatives presents a challenge, so the organisations targeted for input will be selected from the author's network rather than targeting companies at random, thus allowing for more interaction and ensuring a more favourable response.

## 1.5 Delineation and Limitations

### 1.5.1 Scope Inclusions

The scope of research for this dissertation includes IT governance as it relates to:

- The structure of the IT function;
- Principles for defining and segregating IT duties; and
- The management of IT strategy, the IT service lifecycle, information security, IT projects, IT service continuity, enterprise architecture, IT financial management, managing the investment in IT, IT risk, software development quality, IT performance.

### 1.5.2 Scope Exclusions

The scope of the research does not extend to:

- Corporate strategy;
- Physical and all other forms of security, other than information security;
- Enterprise portfolio, programme and project management (only IT project management is included in the scope);
- Business continuity management (only IT service continuity as a sub set is included in the scope);
- Supply chain management and the corporate procurement function (only IT financial management and the management of the investment in IT are included in the scope);
- Enterprise risk management (only IT risk management as a sub set is included in the scope); and
- Corporate performance management (only IT performance management as a sub set is included in the scope).

### 1.5.3 Limitations

The generic IT governance framework formulated is relevant to organisations with a turnover (in the case of private sector companies) or a budget (in the case of Government entities) in excess of R1bn per annum. It is not proposed as an option for smaller organisations.

## 1.6 Assumptions

The following assumptions apply to the research for this dissertation:

- The generic IT governance framework formulated is relevant to any organisation with a turnover (in the case of private sector companies) or a budget (in the case of Government entities) in excess of R1bn per annum;
- IT governance is a priority of all corporate governance agendas;
- All organisations interviewed have some level of IT governance and are willing to consider applying the IT governance framework produced by this research to formalise their IT governance;
- The IT function is critical to the functioning of all organisations interviewed, even to those who do not regard IT as a strategic enabler;
- The proposed IT governance framework is generic and therefore customisable to any environment. Specialised environments, for example in telecommunications companies, could use frameworks like the Enhanced Telecom Operations Map (eTOM) as part of a customised instance of the framework, but the framework will not suggest that such an industry specific be considered for all organisations. COBIT, on the other hand, applies to all organisations and will therefore form part of the proposed framework;
- Business continuity management (BCM) is not a responsibility of the IT function; instead, IT service continuity management (ITSCM), as a sub set of BCM, is the responsibility of IT; and
- The supply chain management function is not an IT governance responsibility, but the management of IT value and, more specifically the manner in which IT complies with procurement policy and expends funds, is the responsibility of IT.

## 1.7 Summary of the Results

The Processes, Enablers and Structures (PES) IT Governance Framework incorporates the elements required to implement an IT governance framework, as required by King III. It utilises popular standards and practices like COBIT 5, ITIL, Prince2 and ISO/IEC27001, through a set of practical recommendations, to enable the implementation of an IT governance framework. The organisations participating in the research confirmed what processes, enablers and structures are feasible for them, in order to refine the theoretical PES IT Governance Framework into a product they would all be able to implement.

The research sucessfully confirmed the feasibility of the proposed PES IT Governance Framework, incorporating participant input and producing a generic IT governance framework that could be applied to any large organisation in South Africa.

One aspect that did not receive the anticipated support and which was therefore not addressed as comprehensively as expected, was the concept of “green” IT, which supports IT sustainability. The research participants consider enabling business to be a going concern as much more important to IT sustainability than green IT.

De Haes (2004:6) states that a framework which is effective in one organisation may not work in the next. It is therefore important that, despite the framework having been accepted by the participants, it is customised for each organisation representing its recommendations.

## 1.8 Thesis Organisation

### Chapter One: Introduction

The introductory chapter provides the research context, the goals of the research, the research methodology followed, delineations and delimitatons applicable to the research, asumptions, and the manner in which research results will be presented.

### Chapter Two: IT Governance and Governance Models

This chapter is structured to review literature on the IT governance and existing IT governance models. It also derives the definitions that are used throughout the subsequent chapters of this research.

### Chapter Three: IT Governance Enablers

Chapter three extends the literature review, covering the practices, standards and frameworks to be considered in formulating a generic IT governance framework. These enablers provide the detail behind the execution of the five IT governance major processes.

### Chapter Four: IT Governance Structures

The final literature review chapter considers the various roles and structures that are accountable and responsible for IT governance. These roles and structures mobilise the IT governance major processes.

### Chapter Five: Proposed New Framework

Based on the literature review, chapter five provides a description of the framework, which is used to prepare a discussion paper for engaging the participating CIOs.

### Chapter Six: Design of the Empirical Work

The design chapter explains the research design and methodology, including the research instruments used, data parameters and analysis techniques. The research limitations are stated.

A specific output of this chapter is the draft discussion paper that will form the basis of interviews with CIOs included in the research process. The paper is based on the outline produced at the end of the literature review.

### Chapter Seven: Results of the Empirical Work and Analysis of the Results

This section of the dissertation lays out the research findings and an analysis of the results, including structured and unstructured input sourced through interviews with CIOs, summaries of analysis of the

CIOs' input, and conclusions on what updates should be made to the proposed IT governance framework.

### Chapter Eight: Final Amended Framework

The end result of the research is an updated framework that reflects the participating CIOs' aggregated feedback.

### Chapter Nine: Conclusion

In the conclusion, the dissertation's research findings are summarised, conclusions drawn, contributors acknowledged, suggestions made for future research (based on trends identified in the preceding chapter), and recommendations made for implementation.

### Appendix

The research discussion paper, which was used to source input from participatig CIOs, is included as an appendix.

# Chapter Two: IT Governance and Governance Models

## 2.1 Abstract

The literature review in this chapter explores IT governance concepts and models. It provides the basis for the subsequent review of IT governance enabler literature and the proposed IT governance framework.

## 2.2 Introduction

In an age where people are recruited based on their Facebook profiles, where paper diaries have become a rarity and no transaction moves without a computer contributing, it is hard to imagine a time when corporate life was not driven by IT. Even large corporates who do not consider IT as strategic have to admit that it is mission-critical. Whether IT is classified as just another support function or a strategic enabler, it has permeated organisations and become crucial to successful business.

In the process, conventional, clear organisational boundaries have become vague, giving rise to the term, "the extended enterprise" (ATOS Consulting, 2007:15), which describes the integration of related enterprises and business functions in the virtual sense, rather than through direct shareholding. E-business has integrated organisations in ways never before contemplated, to the point where some organisations now consider taking IT goverenance beyond their own borders. Technology partner governance extends mere contractual mechanisms for managing relationships to relationship governance, thus covering strategic, operational, financial, commercial and contractual aspects (Ward, 2011:244). To apply the concept of the extended enterprise to IT, this research refers to the extended IT organisation, which implies all IT stakeholders inside and outside the IT function, including those stakeholders external to the organisation.

The fading of corporate and global borders, increasing levels of shareholder activism, and even direct intervention in business by governments gave rise to the question whether corporate governance should be legislated. In the USA, the approach has been more legislative and prescriptive, with the promulgation of the Sarbanes-Oxley Act (US Security and Exchange Commission, 2002) and, more recently, the US government's direct intervention in the management of companies like General Motors. South Africa, in contrast, has opted for a more voluntary adoption of sound governance practices, as laid out in the King Code of Corporate Governance (Institute of Directors Southern Africa, 2009).

As an extension of the enterprise, the governance of IT has become an especially important aspect of corporate governance. Since the 1990s, frameworks like COBIT (ISACA, 2012), ITIL (Wilkinson,

2008) and PMBOK (Project Management Institute, 2004) have contributed to the formalisation of the IT governance body of knowledge, to a point where there are now so many tools to choose from that organisations sometimes find it difficult to bring them together into a single IT governance framework.

In 2008, the American Institute of Certified Public Accountants listed IT governance, information security management, disaster recovery, privacy management, and identity and access management among its top ten technology areas likely to have the greatest impact on organisations (Filipek, 2008:16). On the other hand, Mahoney (2008:10) believes that the four closely related disciplines shaping the future of IT are architecture and strategy, service management, governance and risk management, and leadership of transformation.

IT governance depends on sound corporate governance, which necessitates the IT leadership's understanding of corporate governance and how to involve senior business in IT governance (Gerrard, Short, 2009:1). Inadequate Board oversight of IT activities has the potential of creating significant risk to the enterprise (Gerrard, Short, 2009:4). Where organisations regard IT as strategic, the need for Board involvement increases and boards require assurance that IT is aligned with business strategy (Gerrard, Short, 2009:5). Despite this, a number of researchers concur that there remains limited understanding of the role of the Board in IT governance (Jewer, McKay, 2012). Jewer and McKay continue to argue that enterprise governance of IT is an integral part of enterprise governance, addressing the formalisation of processes, structures and relational mechanisms in the organisation that facilitate active participation and collaborative relationships among executives, IT management, and business line management.

This literature review considers various IT governance frameworks and practices, leading to a generic framework that could be applied to large organisations. Such a framework is required because, as shown in the Introduction to this research, no universally appropriate, contemporary IT governance framework or a single, cohesive view of IT governance exists, and there is a lacking understanding of the concept of an IT governance framework.

## 2.3 Definitions

### 2.3.1 Desirable Practice

According to the Canadian Oxford Dictionary (Barber, 2004), a best practice is defined as, "that practice which is most appropriate, esp. that practice in the conduct of commercial or professional activities which is accepted by consensus or prescribed by regulation as being correct" (Barber, 2004).

Hoske (2009:31) describes a de facto standard as one used by so many people that it is almost a standard without a standards body. Freschi (2009:48) defines a de jure standard as one that is approved by a recognised standards organisation, for example the International Standards Organisation (ISO), and a de facto standard as one being dominant enough that the industry follows it as if it were an authorised (de jure) standard.  According to Freschi, de facto standards usually belong to one or a limited number of companies.  Oud (2005) makes the statement that standards in most countries are de facto, with IT management and IT security standards following or in themselves constituting best practices.

To avoid unnecessary debate as to whether a practice or standard is the best or only option for a particular aspect of IT, the term “desirable practice” will be used in this dissertation.  Considering all of the above, this research uses the following definition for desirable practice: The most appropriate practice accepted by consensus as a de facto standard or through certification as a de jure standard.

### 2.3.2 IT Governance

Various authors have provided their own interpretations of the term “IT governance”.  These were considered before formulating the definition that will be used throughout the dissertation.  The third King Report (“King III”) on Corporate Governance considers IT governance to be “a framework that supports effective and efficient management of IT resources to facilitate the achievement of a company’s strategic objectives”. It considers this one of the responsibilities of the Board (Institute of Directors Southern Africa, 2009:82).

The IIA's International Professional Practices Framework defines IT governance as, “the leadership, organisational structures, and processes that ensure that the enterprise's information technology supports the organisation's  strategies and objectives” (Reinhard, 2013).

Forrester (2007:3) defines IT governance as, the “… act of establishing IT decision structures, processes, and communication mechanisms in support of the business objectives and tracking progress against fulfilling business obligations efficiently and consistently.”

The IT Governance Institute (ITGI) arguably publishes most material on the topic of IT governance, which it regards as, “… the responsibility of the Board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation’s IT sustains and extends the organisation’s strategies and objectives” (IT Governance Institute, 2003: 10).

The ITGI (2003:19) continues to list five main focus areas for IT governance, namely: strategic alignment, resource management, risk management, IT value delivery, and performance measurement.

Robertson (2006:119,121-122) regards IT governance as the “decision rights and accountability framework to encourage desirable behaviour in the use of IT”. It continues to state that “... IT governance might share mechanisms, such as executive committees and budget processes, with other asset-governance processes, thereby aligning company-wide decision-making processes."

Raghupathi (2007:95-96) bases his IT governance definition on his views of corporate governance by focusing on three questions: dealing with ensuring return on IT investment, the role of the CIO, and control of the IS function controlled by top management.

Pollard (2006:7) states that "IT Governance is the strategic alignment of IT with the business such that maximum business value is achieved through the development and maintenance of effective IT control and accountability, performance management and risk management".

Boulton (2008:68) emphasises responsibilities for IT investment and related approval authority in his view of IT governance.

Bamberger (2006:56) calls IT governance "the orchestration between management and the IT governance team". He also emphasises the role of effective IT policies and procedures to govern behaviour.

Peterson's definition is that "IT governance is thus the enterprise management system through which an organisation's portfolio of IT systems is directed and controlled" (Peterson, 2004:8).

IT governance means specifying the framework for management rights and accountabilities regarding IT related decisions (ATOS, 2007:7).

In Sandrino-Arndt's view (2008:1), IT governance is a set of formal and informal rules and practices that determine the manner in which IT decisions are made, and how the execution of those decisions is monitored and measured. It further includes how decision making is empowered and how accountability for decisions is enforced.

TOGAF states that IT governance "provides the framework and structure that links IT resources and information to enterprise goals and strategies. Furthermore, IT governance institutionalises best practices for planning, acquiring, implementing, and monitoring IT performance, to ensure that the enterprise's IT assets support its business objectives" (Capgemini, 2008:651).

The National Computing Centre (NCC) explains the contribution of IT governance to corporate governance as follows: "IT has a pivotal role to play in improving corporate governance practices, because critical business processes are usually automated and directors rely on information provided by IT systems for their decision making" (National Computing Centre, 2005:4). The NCC (2005:7) continues to recommend the implementation of an IT governance and control framework as best practice.

An IT control framework defines the underlying structure of the IT internal control environment, including all the most significant controls for the IT environment, together with the complementary, supporting controls.

The following, composite definition of IT governance will be used in this research: IT governance is that sub set of corporate governance dealing with the structure of the IT organisation and its mechanisms for effectively supporting the IT governance major processes.

### 2.3.3 IT Governance Model

The Collins English Dictionary (Collins, 2015) defines a model as a theoretical description that helps one understand how a process might work. An IT governance model may thus be viewed as a theoretical desciption of how an IT governance process might work.

Breslin (2011) defines a model as a simplified representation or description of a system or complex entity. Applying this definition to IT governance, one might view an IT governance model as a simplified description of IT governance processes.

The Cambridge Dictionary (2015) defines a model as something that represents another thing. In the case of IT governance, the model depicts the underlying process structure for governing IT.

The ITGI model for IT governance (IT Governance Institute, 2003) could be used as an example of the application of each of the above definitions, as it describes how the five processes migt be used to explain how IT governance theory may work; it reduces and simplifies IT governance to understandable processes; and its pentagon depicts the underlying processes for governing IT.

### 2.3.4 IT Governance Framework

The Concise Oxford English Dictionary (2008) defines a framework as: “an essential supporting or underlying structure”. King III (Institute of Directors of Southern Africa, 2009:82) requires an IT governance framework to include relevant structures, processes and mechanisms to enable IT to deliver value to the business and mitigate IT risk. Symons (2008:4) applies similar thinking to describe and IT governance framework as consisting of governance structures, processes, measurement and communications.

Bloem states that an IT governance framework must “help to set the appropriate priorities, must be easy to use without requiring people to manipulate the system, must link strategy to the desirable behaviour, and must fit inside your complete organisational management” (Bloem, 2006:251). De Haes emphasises the need for “a variety of structures, processes and relational mechanisms” in an IT governance framework (De Haes, 2004:6).

The Cambridge Dictionary (2015) provides a simple, yet useful definition of a framework as a supporting structure around which something can be built. In the case of IT governance, the framework for governing IT.

Combining the above thinking with the definition of IT governance, the following definition of IT governance framework will be used in this research: an IT governance framework is the underlying structure supporting IT governance through the combination of governance structures, architecture, processes, desirable practices and an IT control framework to effectively support the IT governance major processes.

### 2.3.5 Office of the CIO

The term "Office of the CIO" refers to the IT leadership reporting to the CIO, who provide services outside applications and infrastructure (Cecere, 2009:1).

## 2.4 Background on IT Governance

Many opinions are available on what exactly constitutes IT governance. The absence of effective IT governance mechanisms could significantly impact organisations. An example of this would be the case of the former Societe Generale trader, Jerome Kerviel (CNN, 2010), who exposed the bank to transactions through unauthorised access to systems. This could be interpreted as indicative that the bank's information security controls were inadequate, which reflects on the effectiveness of management's system of internal IT control.

Achieving effective IT governance should never be a goal in itself; it needs to be subservient to corporate governance, which IT governance should support to achieve corporate goals. An attempt at legislating corporate governance in the case of the Sarbanes-Oxley Act in the USA has resulted in control improvements which do support better corporate governance but which have not prevented a number of large corporate failures since their introduction. Sarbanes-Oxley focused mostly on financial control effectiveness, with IT controls being required more implicitly, in support of the financial controls. The legislation has, in effect, improved financial controls, including the related IT controls, but has not significantly benefited other aspects of IT governance.

King III, which is a much more recent publication, spells out explicit IT governance requirements to support effective corporate governance practices. Aside from its South African focus, this arguably makes King III the most useful publication to date on IT governance in relation to corporate governance. As the first international standard on IT governance, ISO/IEC38500 (2008) is a milestone in itself, but has not achieved general acceptance and still falls short of providing the detail required for implementation, such as that provided by ISO/IEC27001 (2005). The next section compares King III to ISO/IEC38500, reducing the two publications to a set of key implementation requirements for any future IT governance frameworks.

It should furthermore be recognised that IT governance is largely dependent on the quality of leadership which the CIO provides, as well as the attitude of the organisation toward corporate governance. In practice, a common challenge to IT functions is not to become caught up in the deployment of individual desirable practices or IT governance tools at the expense of a comprehensive, holistic IT governance framework.

### 2.4.1 IT Governance Major Processes

The IT Governance Institute (ITGI) offers a simple, practicable IT governance model, comprising five pillars (2003), namely: strategic alignment, value delivery, risk management, resource management, and performance management. For the purposes of this research, the five pillars are presented as the IT governance major processes.

The large amount of IT governance material published by the ITGI, and their influence on the structure of COBIT, which is explored below as a desirable practice for IT control objectives, influenced the decision to adopt the five processes from the ITGI model (IT Governance Institute, 2003). In performing this literature review, it was found that the ITGI is the single largest publisher of IT governance books and articles and that, via the Information Systems Audit and Control Association (ISACA), which has a large membership of IT governance professionals, the ITGI publications are most accessible to professionals and practitioners of IT governance literature. Using the ITGI model, this paper also references other ITGI publications supporting the model, for example, COBIT and ValIT, to maintain the ITGI process context.

The IT governance enablers and IT governance structures support the implementation of each of the five IT governance major processes. The substance of these processes will become clear as the reader progresses into the Enablers and IT Governance Structures sections.

The two remaining sections (Enablers and IT Governance Structures) are referenced back to the five processes to achieve the effect of an integrated view of the framework. The five major processes are described below.

#### *2.4.1.1 Strategic Alignment*

Strategic alignment requires IT objectives (and accordingly, the IT strategy), IT operations and investment in IT to support the achievement of organisational objectives. When organisational objectives change, IT must adjust its objectives accordingly (IT Governance Institute, 2003:22-24). In its most basic form, strategic alignment of IT to organisational objectives starts with IT strategic planning. Functional strategy at the IT departmental level should be aligned to grand strategy at the organisational level, and action plans formulated to ensure that IT contributes to successful implementation of organisational strategy (Ehlers, Lazenby, 2004:149).

Enterprise architecture and IT portfolio management, which are described in more detail in the Enablers section, provide valuable mechanisms for aligning IT to business. Enterprise architecture is considered a means of ensuring that structures, processes, systems and infrastructure are aligned to organisational objectives, while IT Portfolio Management is considered a means of ensuring that projects and services are aligned to organisational objectives. Bodies involved in monitoring the strategic alignment of IT include the Enterprise Architecture Forum, the IT Strategy Committee and the IT Steering Committee.

In the IT context, sound governance requires the alignment of IT strategy, planning, investment and operations to technologically enable departments contributing to strategic objectives. This is achieved by implementing a performance management process, which includes the formulation of IT objectives with related key performance indicators (KPIs) that make it clear how IT would enable these departments to achieve their objectives. Combining IT strategy maps with a performance scorecard (Kaplan, 2006:146) is one effective way to conceptualise the IT service cycle from strategy to delivery. In Strategy Maps, Kaplan (2004:13) also lists the strategic IT portfolio as one of three mechanisms to align intangible assets to strategy, in this instance, information capital to strategic themes. IT resource management, application of balanced scorecards, knowledge sharing and IT architecture contribute to better alignment between IT and business (Motlagh, Sabegh, 2012). De Haes and Van Grembergen[b] (2009) found that organisations which manage to achieve alignment between business and IT usually demonstrate a higher level of maturity.

#### 2.4.1.2 Value Delivery

To many, the focus of value delivery is on return on investment, that is, does the investment in IT yield the return expected at the point of committing to the investment? In reality, however, finding a simple, easily understood investment value calculation is not realistic, and reducing the value question to return on investment metrics portrays a very limited view of value (Silvius, 2011).

The ValIT Framework, originally published by the IT Governance Institute during 2006, provides a useful structure for value delivery, comprising value governance, portfolio management and investment management. "ValIT supports the business goal of realising optimal value from IT-enabled business investments at an affordable cost with an acceptable level of risk" (IT Governance Institute, 2008). It is still relatively new and few South African organisations have adopted it, but long-term IT governance frameworks cannot afford to ignore it.

An important mechanism for delivering value is the Service Level Management Process (Office of Government Commerce, 2001), which manages and monitors service delivery in accordance with the service strategy and design. Service Level Management is a Service Delivery process, included in the IT Infrastructure Library (ITIL). As a vehicle for facilitating value delivery, the Programme Management Office (PMO) is a structure that translates IT strategy into execution. Where IT organisations are most successful at delivering value, IT governance practices are often embedded within broader corporate governance. This manifests in areas such as project portfolio management, where the enterprise and IT processes are aligned or formally integrated (Bloch, Hoyoz-Gomez, 2009:35). Sometimes overlooked as a value delivery enabler, enterprise architectural competency presents a critical part of value delivery (Brown, Grant, 2005:142).

#### *2.4.1.3 Resource Management*

COBIT identified four IT resource categories, including: applications, information, people, and infrastructure (IT Governance Institute, 2007:12). COBIT, as a desirable practice for IT internal controls, is discussed in the Enablers section below. Formal IT processes are required to manage these resources and are supported by policies, procedures, standards, methodologies and an internal IT control framework. To formalise IT processes within the operational COBIT domains, the desirable practices discussed in the Enablers section should be applied. Specific enablers supporting resource management are IT service management, project management (monitored via a PMO) and information security management. The management roles identified in the IT Governance Structures section are the ones responsible for resource management.

#### *2.4.1.4 Risk Management*

IT risk management focuses on three processes, namely: Risk Governance, Risk Evaluation and Risk Response, in order to:

- Set responsibility for IT risk management;
- Set objectives and define risk appetite and tolerance;
- Identify, analyse and describe risk;
- Monitor risk exposure;
- Treat IT risk; and
- Link with existing guidance to manage risk (IT Governance Institute, 2009).

The RiskIT exposure draft was the IT Governance Institute's first step in establishing a formal directive on IT risk management, as a complementary publication to COBIT and ValIT. RiskIT provides a mapping between COBIT and the IT risk management process. The traditional view of IT risk management has often emphasised information security management and IT service continuity management. When comparing Risk IT, ITIL (specifically the IT Service Continuity Management Process) and ISO/IEC27001 (Information Security Management Process), it becomes clear that more or less the same process could be followed for identifying and analysing risk pertaining to any aspect of IT.

IT risk management programmes are often not aligned to enterprise risk management (CMA Management, 2008). IT risk management requires IT risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise, embedding of IT risk management responsibilities into the organisation, and defining IT risk in the context of the enterprise risk management (ERM) process. Effective IT risk management is only possible as a sub set of the overall enterprise risk management process. Conversely, all line managers who rely on IT should contribute to IT risk management (Datamonitor, 2007). Treating IT risk management as a technology rather than a business issue threatens more than just the effectiveness of IT (Datamonitor, 2008).

EY rates emerging technologies among the top ten in its global risk ratings from 2013 through 2015. These include cloud computing, mobile applications and big data. Emerging technologies are increasingly seen as areas of opportunity rater than threat (EY, 2013:4;34). Rather than deal with these topics as specifics in the IT governance framework, it would be desirable to provide for a comprehensive framework that addresses IT risk management in the broad sense, instead of focusing on specific risks.

#### *2.4.1.5 Performance Measurement*

Performance measurement monitors strategy implementation, project completion, resource usage, process performance and service delivery (IT Governance Institute, 2007:6). Balanced scorecards monitor the translation of strategy into action. The ITGI proposes the implementation of an IT balanced scorecard incorporating enterprise contribution (the manner in which business executives view IT), user orientation (the user view of IT), operational excellence (effectiveness and efficiency of the IT processes) and future orientation (how well IT is positioned to meet future needs) (IT Governance Institute, 2003:29). The balanced scorecard paragraph in the Enablers section discusses this mechanism and should be referenced for more details on performance measurement.

### 2.4.2 ISO/IEC38500

ISO/IEC38500 provides directors of organisations with a framework of principles for the effective, efficient and acceptable use of IT in their organisations (ISO, 2008:1). It is the first formal ISO standard on IT governance. The standard sets out six principles for "good corporate governance of IT", which deal with the following: allocation of responsibility, IT strategy, making acquisitions with business value in mind, IT performance to the agreed service levels, conformance with legislation and regulations, and respect for human behaviour or "the people in the process".

#### Strengths and limitations of practice

The standard follows and globalises the related, pioneering Australian standard AS-8015 Corporate Governance of Information and Communications Technology and is likely be accepted and implemented globally. At this stage the standard is still limited to a set of principles and does not include detailed guidance on their implementation.

#### Impact on a generic framework

The only potential alternative to ISO/IEC38500 would be Australian standard AS-8015, but due to its geographic reach it is not considered a viable alternative. The principles which ISO/IEC38500 stipulates are general and touch on all aspects of the most basic IT governance infrastructure, which would anyway be requirements of a generic IT governance framework.

### 2.4.3 King III Report

The King Report on Governance for South Africa 2009 ("King III") is relevant to all South African companies, in particular those companies listed on the Johannesburg Stock Exchange. New listing requirements and potential future corporate financial reporting standards are expected to contain a statement of compliance with King III, which now includes a section dedicated to IT Governance. The IT governance requirements of King III are set out in a separate chapter (five) and can be summarised as follows (Institute of Directors Southern Africa, 2009:81-87):

- The Board is responsible for IT governance;
- IT should be aligned to the company's sustainability and performance objectives;
- The Board should delegate the responsibility for implementing an IT governance framework to management;
- The Board should monitor significant IT expenditure and investments;
- IT should be considered integral to risk management;
- The Board is responsible for ensuring the effective management of information assets; and
- Risk and audit committees should help the Board execute its IT responsibilities.

#### Strengths and limitations of practice

Large South African organisations, especially companies in the private sector, should expect that future compliance requirements will include proof that the IT governance requirements in King III have been met. The IT Governance chapter would have had even more impact, however, if it showed clearer alignment to ISO/IEC38500.

#### Impact on a a generic framework

ISO/IEC38500 provides a formal alternative to the King III IT governance chapter, although listed South African companies would in future be required to comply with King III. On the other hand, compliance with King III could largely be achieved through compliance with ISO/IEC38500. As the authoritative work on corporate governance for South Africa, it is without doubt an important determinant of compliance with local corporate governance requirements.

### 2.4.4 King III and ISO/IEC38500 as Foundations for IT Governance

The past few years saw two significant publications that no listed South African company or Government organisation can ignore in its approach to practising IT governance. The third King report on corporate governance in South Africa ("King III") has become a requirement for the larger players in corporate South Africa, while over the longer period, the first international standard on IT governance, ISO/IEC38500 could become the global reference on IT governance fundamentals. As a requirement for all listed entities, chapter five of King III sets out the IT governance principles that must be incorporated into any South African IT governance framework. In order to determine what apects of ISO/IEC38500 are not addressed by King III and also need to be incorporated into a generic framework, a comparison between chapter five of King III and ISO/IEC38500 is presented in Table 2.1 below, together with the practical implementation requirements.

| ISO/IEC38500 requirement | King III requirement | Implied requirements |
|---|---|---|
| Principle 1 – Responsibility: All role players understand and accept their responsibility for IT supply and demand and are empowered to meet their responsibilities. | The Board should delegate the responsibility for IT governance implementation to management. | 1. Establishment of IT Steering Committee to oversee IT investment, priorities and resource allocation, on behalf of the Board; and<br>2. Making the CIO the single point of accountability for IT to the Steering Committee. |
| Principle 2 – Strategy: The organisation's business strategy takes into account the current and future capabilities of IT; the strategic plans for IT satisfy the current and ongoing needs of the organisation's business strategy. | The Board is responsible for ensuring effective IT governance. | 3. Establishment of IT Strategy Committee or combined IT strategy and Steering Committee to involve the Board in strategic IT decisions.<br>4. Implementation of a comprehensive IT governance framework. |
| Principle 3 – Acquisition: IT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision making. There is appropriate balance between benefits, opportunities, costs and risks, in both the short term and the long term. | The Board should monitor and evaluate significant IT investments and expenditure. | 5. Compliance with corporate procurement policy, procedures and standards for high-value acquisitions. Where feasible, an IT vendor management process should be implemented.<br>6. Monitoring of significant investments by the IT Steering Committee for value in terms of IT strategy and |

| ISO/IEC38500 requirement | King III requirement | Implied requirements |
|---|---|---|
| | | appropriateness of resource allocation to the investment; also monitoring compliance with procurement policy.<br>7. Implementation of IT project portfolio management to track the value derived from IT investments or at least a basic IT value management process. |
| Principle 4 – Performance: IT is fit for purpose in supporting the organisation, providing the services, levels of service and service quality required to meet current and future business requirements. | IT should be aligned with the performance and sustainability objectives of the company.<br>The Board should ensure that information assets are managed effectively. | 8. Implementation of a procedure for the continual re-alignment of the IT objectives to those of the organisation.<br>9. Implementation of regular performance reporting by IT to the IT Steering Committee to monitor the execution of the IT strategy and IT service delivery in general. |
| Principle 5 – Conformance: IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced. | IT should form an integral part of the company's risk management | 10. Implementation of a formal IT risk management function, with the CIO being accountable for effective IT risk management and a specific person being responsible for ensuring that the required IT risk management practices are followed.<br>11. Implementation of a risk assessment process that requires at least an annual, comprehensive IT risk |

| ISO/IEC38500 requirement | King III requirement | Implied requirements |
|---|---|---|
| | | assessment and regular updates to the IT risk understanding, all of which are documented and monitored in a formal IT risk register. |
| Principle 6 – Human Behaviour: IT policies, practices and decisions demonstrate respect for human behaviour, including the current and evolving needs of all the "people in the process". | IT should form an integral part of the company's risk management. | 12. Implementation of a set of policies, procedures and standards guiding behaviour in IT, in line with the organisational objectives. |
| No direct mapping to King III. | A risk committee and an audit committee should assist the Board in carrying out its IT responsibilities. | 13. Allocation of a fixed reporting slot for IT-related matters on the agendas of all risk and audit committee meetings. |

**Table 2.1 – King III and ISO/IEC38500 Comparison**

The key implementation requirements identified above would apply to any implementation of an IT governance framework, regardless of the selected framework. Conforming with Chapter Five of King III, South African companies find themselves addressing more than the seven IT governance principles. By implementing an IT governance framework they in fact incorporate several practices and standards that usually go beyond King III (Butler, Butler, 2010). Internationally, Board involvement remains a challenge, as many boards still only consider IT matters on an ad hoc basis (Romero, 2012). King III has at least brought IT governance onto the agenda of South African boards.

### 2.4.5 IT Governance Models

This section explores existing IT governance models, compares the models to identify common characteristics and strengths, and then summarises the commonalities. The researcher considered six IT governance models, together with King III and ISO/IEC38500, which were discussed above.

The 3P model (Sandrino-Arndt, 2009) comprises three perspectives, namely: people, portfolios, and processes, and focuses on the structural aspects of implementing an IT governance model. The work of Weill and Ross (Robertson, Ross, Weill, 2006) related to enterprise architecture is often referenced in the IT fraternity. Their view of IT governance (2009:90) focuses on decision rights and accountabilities. It incorporates five key decision areas and five IT mechanisms for enforcing IT governance. Costello and Laplante (2006:298) propose that the CPR Framework for Corporate Governance be applied for IT governance purposes. The three components of the framework are: conformance, performance and relating responsibility. The Forrester model (Kark, Othersen, McClean, 2007:3) differentiates among IT governance, IT risk management and IT compliance and offers a more comprehensive option than most of the other models and frameworks considered. The ATOS Consulting model (2007) addresses IT governance in the extended enterprise. The research model proposed by Brown and Grant (2005:696) suggests that IT governance often represents the weakest link in a corporation's overall governance structure. They reduce IT governance to a set of decision-making structures and position the model in a way that supports academic research. Except for King III, which mentions it specifically, none of these models addresses sustainability. A discussion of each model follows.

#### 2.4.5.1 3P Model

The 3P model is based on the premise that IT governance is about IT decision-making rights and responsibilities. The model comprises the following three perspectives:

i) People perspective – structures, roles and responsibilities (Sandrino-Arndt, 2009:3): The People perspective identifies existing governance mechanisms and their roles in the decision-making process. Furthermore, it compares the decision-making processes and mechanisms to the objectives of the IT governance project and identifies gaps in structures, processes and mechanisms. This perspective emphasises the view that IT governance is about decision-making rights and responsibilities, which demonstrates an inadequate understanding of the topic.

ii) Portfolio perspective (Sandrino-Arndt, 2009:5): The Portfolio perspective defines the focal areas for governance measures to be applied in future. This perspective is poorly described and does not clearly bring out the need for value or benefits management as part of the portfolio management process. It is vague and only touches on the categorisation and creation of an inventory for IT projects.

iii) Process perspective and decision-execution monitoring (Sandrino-Arndt, 2009:5): The Process perspective defines IT governance mechanisms and rules, designs policies and procedures, defines and implements process-specific roles, and designs templates and tools for the IT governance implementation project. It does not provide guidance on typical mechanisms and processes that could be expected in an effective IT governance infrastructure.

The model focuses on implementing IT governance decision-making rights and responsibilities, following five steps (Sandrino-Arndt, 2009:1-3), namely:

i) Identifying business drivers: This step establishes the motivation for the project and defines the expected business outcomes of the IT governance project.
ii) Assessing organisational readiness: Organisational structures and processes are evaluated to identify weaknesses and set improvement targets. Key stakeholders are identified and their potential support secured.
iii) Defining implementation goals: Stakeholders are engaged in discussions about the desired future state of IT governance in the organisation, the project scope is identified, stakeholder commitment to the project is secured, and implementation planning is finalised.
iv) Implementing IT governance plan: The IT governance processes and structures are implemented, according to the 3P model, that is, the portfolio, process and people aspects. Once the implementation has been completed, a post implementation review is performed.
v) Operationalising the governance processes: The communication campaign is launched to communicate timelines, while training workshops are run to familiarise everybody with the "to-be processes".

This model could be useful when planning the approach to an IT governance implementation but is of limited use when formulating an IT governance framework.

#### *2.4.5.2 Weil and Ross*

The Weill and Ross (2009:90) view of IT governance is that it involves IT decision rights and accountabilities, which demonstrates a limited view on the scope of IT governance. Under the Weill and Ross model, decision rights and accountabilities are allocated to at least five areas (Ross, 2009:91-92), namely:

i) IT principles: Ross's view is that IT principles relate to the operating model of the organisation and any directives clarifying the role of IT in the organisation. IT governance addresses the allocation of decision rights to senior management for determining IT principles. This is too vague and is addressed in more detail by the specific roles and responsibilities discussed in subsequent sections of this literature review.
ii) Enterprise architecture: Enterprise architecture refers to the design of the electronic platform. IT governance specifies who is responsible for establishing business processes, data and technology standards, and for dealing with requests for deviating from these standards. Enterprise architecture forms an important part of an IT governance framework and is discussed later in this document.
iii) IT infrastructure: Ross uses the term IT infrastructure to refer to shared IT services across the organisation. IT governance deals with the allocation of responsibility for defining, providing and pricing shared IT services. IT shared services is not a concept applicable to all organisations and

falls under a generic shared services concept. As it is not IT-specific and not a topic that could be generalised for IT, it will not be covered further by this research.

iv) Business needs and project deliverables: This area covers the establishment of new processes and systems. IT governance allocates the ownership for business case definition, governance over the implementation, up to the point where project benefits have been realised. This area is appropriately addressed by enterprise architecture and the programme management office, both of which are discussed later in this document.

v) IT investment and prioritisation: This area covers IT portfolio management, including the prioritisation of fund allocations and metrics for monitoring IT spend. IT governance therefore addresses decision making over IT portfolio management and allocation of funding. IT portfolio management is discussed later in this document.

Ross identifies five mechanisms commonly found in organisations with effective IT governance, namely:

i) Senior management committee: A senior management committee that includes some or all of the organisation's top executives governs IT decision making, including laying down IT principles and spending and prioritisation. This correlates with the idea of having an IT Steering Committee, which is discussed later in this literature survey.

ii) IT leadership team: The CIO leads a team comprising IT leadership, who have substantial IT decision-making responsibilities over enterprise standards, IT infrastructure and shared services. This thinking is similar to that of having an Office of the CIO, which combines with a wider group of IT management staff to lead the IT function.

iii) Business-IT relationship managers: Relationship managers are responsible for linking business with IT needs, and engage at a level below senior management to facilitate this. Although they play a valuable role in the effectiveness of IT, this is not regarded as a key requirement for effective IT governance, as they are more junior and not part of the core IT management team or any other senior IT governance structure.

iv) Management/oversight of IT projects and services: A PMO designs the project methodology and provides project oversight. The role of the PMO is a key component to effective IT governance and is discussed later in this literature survey.

v) Tracking the business value of IT: The value of IT spend has been problematic for decades (Marks, 2010). Post implementation reviews represent one useful method of tracking the value of IT, as well as learning how to generate value from IT. As post implementation reviews and project benefits management are part of the function of the PMO, they will not be treated separately from the PMO in this research.

Weill and Ross have contributed a great deal to establishing IT architecture concepts and to raising awareness of IT governance, though their model needs to be expanded to constitute a proper IT governance framework.

#### *2.4.5.3 CPR Framework*

Costello (2006:298) proposes the conformance, performance and relating responsibility (CPR) framework for corporate governance as an option for IT governance. This framework focuses on four primary asset themes, namely: infrastructure, clients and external stakeholders, internal (people and process), and value creation. It relates the CPR concept back to these assets.

The three elements of CPR are discussed below:

i) Conformance: Costello (2006:294) explains that conformance is about complying with the authorities to minimise business risk. The proposed mechanisms for achieving this is a key performance indicator (KPI) dashboard. This covers the typical compliance view that is expected in IT governance models, though it only includes external compliance while ignoring internal policies, procedures, standards and the internal control framework.

ii) Performance: The performance element emphasises effectiveness and efficiency of IT resources, which Costello (2006:295) proposes should be measured through a KPI dashBoard and "assessment review". It does not contextualise this element in relation to corporate performance management or even some corporate score card.

iii) Relating responsibility: This element covers the organisational values, corporate responsibility and other "soft" aspects of governance (2006:295).

Costello argues that the CPR could be implemented for IT by adhering to the following principles:

i) The Board must drive IT governance and the establishment of an IT governance framework. This principle aligns well with King III but also shows that CPR is at best a model to be used in formulating an IT governance framework and not a framework in itself.

ii) IT governance must contribute to sustained financial results. This principle demonstrates an incomplete understanding of corporate and IT governance which, in the modern era, not only focuses on financial results.

iii) IT governance must govern the four asset themes according to the three CPR dimensions for the current and future state of the business.

iv) Governance is about behaviour, and implementing the CPR framework for IT governance should focus on changing behaviours. While this is a valid point as far as the implementation of IT governance frameworks is concerned, this dissertation focuses on the framework itself rather than its implementation.

v) Other IT governance frameworks, for example ITIL and activities must be aligned within the framework. Costello is not clear about what he means by this. A framework should do this inherently.

As a framework, this view lacks many elements that are expected, yet it includes useful detail on some practices to be implemented to create IT governance mechanisms. It would have been more complete if IT risk management, strategic alignment and value management had been included.

#### 2.4.5.4 Forrester

Forrester (Kark, 2007:1) defines IT governance as a discipline distinct from IT risk management and IT compliance. This follows a popular trend to refer to governance, risk and compliance (GRC), but goes against most of the authoritative IT governance literature, most notably the publications of the IT Governance Institute. For the purposes of this research, IT risk management and IT compliance will be regarded as sub sets of IT governance.

The Forrester model (Kark, 2007:3) comprises three segments, namely:

i) IT governance: Forrester defines IT governance as the act of establishing IT decision structures, processes, and communication mechanisms supporting business objectives and tracking progress in fulfilling business obligations efficiently and consistently. It comprises structures (organisations, committees, informal structures, roles and responsibilities), communication (strategy and principles, policies, goals and deliverables, service levels) and process (prioritisation, approval, operational) governance.

ii) IT risk management: Forrester sees IT risk management as a coordinated set of activities to manage the adverse impacts of IT on business operations and to realise the opportunities that IT brings to increase business value. It encompasses IT operational risk (information security, IT resilience), technology (agility, architecture) and IT business partner (vendor management, third parties) risk management.

iii) IT compliance: Forrester defines IT compliance as a process of establishing appropriate controls for the IT environment and managing the implementation of those controls. This involves best practice (best practice compliance, standard/framework compliance), corporate compliance (human resources, security and privacy), and legal and regulatory compliance (industry and global regulations, as well as local and global legislation).

The approach Forrester recommends to aligning the IT governance, risk and compliance silos includes: understanding dependencies and providing a common approach; unifying controls for IT risk and compliance; enabling IT governance by establishing accountability; and aligning technology and process for efficiency and consistency. The Forrester model is too high-level to be of real value to the establishment of a generic IT governance framework and places too much emphasis on IT risk management and IT compliance, apart from IT governance.

#### *2.4.5.5 ATOS Consulting*

The ATOS model views IT governance as the means for specifying a framework for management rights and accountabilities about decisions affecting IT (ATOS, 2007:5). The model includes three activity classes, namely: align, arrange and perform.

i) Align deals with strategic IT decisions, including those on strategy, architecture, infrastructure, application needs and IT investment. The question here is what IT decisions are required to ensure effective management and IT utilisation (ATOS, 2007:15)?

ii) Arrange covers the IT governance structures, including positioning structures, the decision-making process and coordination mechanisms. IT addresses the question – who will have to make the decisions?

iii) Perform is about meeting the critical success factors for IT governance. How can these decisions be made and how can they be monitored?

The idea behind the model is to govern the manner in which IT interacts across formal organisational boundaries. However, it has limited reach in terms of being a comprehensive IT governance framework.

#### *2.4.5.6 Brown*

Brown and Grant (2005:696) opines that IT governance often represents the weakest link in a corporation's overall governance structure. Brown and Grant (2005:700) views IT governance models as a combination of structural forms, that is, whether the IT department's decision-making structures are centralised, decentralised or federal; and contingency analysis, that is, understanding the single and multiple contingencies influencing the adoption of particular individual governance forms. The underlying perception is that IT governance is about decision-making structures. This attempt to establish a framework for IT governance research over-simplifies the topic and offers little along the lines of a practicable IT governance framework, or even the theoretical foundation for such a framework. Brown and Grant emphasise the importance of Weill and Ross's work in researching IT governance (Brown, Grant, 2005:709). Brown and Grant's work largely ignores the IT Governance Institute's work, instead selecting older schools of thought ranging back to 1957. This renders the work of limited use.

### 2.4.6 Comparative Summary of IT Governance Models

Having discussed the six IT governance models, a comparative summary is presented in Table 2.2 below, considering applicability of the model and common elements, as well as the positive and negative aspects of each.

|  | 3P model | Weil and Ross model | CPR framework | ATOS Consulting model | Forrester model | Brown's model |
|---|---|---|---|---|---|---|
| Applicability | An approach to implementing IT governance structures and processes, without regard for detail or desirable practice. | IT governance, in the context of enterprise architecture. | IT governance, as a sub set of corporate governance, to achieve financial organisational objectives. | Extended enterprise governance, that is, IT governance within partnerships. | IT governance, risk and compliance (GRC). | A logical structure for reviewing existing IT governance research. |
| Common elements | Structure: roles, bodies, functions.<br>Process: portfolio management process, policies, procedures, standards. | Structure: mechanisms, roles, bodies, functions. | Process: measurement processes and related KPIs. | Structure: IT governance structures.<br>Process: strategic alignment process, performance management process. | Structure: roles, bodies.<br>Process: IT risk management, IT compliance, policies, legal and regulatory compliance. | Structure: departmental structure. |
| Positives | Applicability to implementations regardless of the practices deployed by the implementation. | Weill and Ross are well-respected among enterprise architecture and IT governance professionals. | The framework emphasises the fact that IT governance only makes sense in the wider corporate governance context, thus ensuring that IT governance projects do not exist in isolation from the wider perspective. | Most publications focus internally only. This model makes provision for inter-organisational IT governance. | Of all the models considered by this literature review, this is the most comprehensive. | Academic research models for IT governance are not common; this framework provides an academic perspective. |

| | 3P model | Weil and Ross model | CPR framework | ATOS Consulting model | Forrester model | Brown's model |
|---|---|---|---|---|---|---|
| Negatives | The people perspective of this model does not adequately explain how strategy and architecture roles fit in.<br>The model does not explain the role of the CIO or clarify specific management roles in the IT department.<br>The portfolio perspective (Sandrino-Arndt, 2009:5) takes a narrow rather than comprehensive view of IT portfolio management as a means of identifying and categorising IT projects, whereas IT portfolio management should be used as a strategic alignment tool incorporating both IT programmes and services.<br>The portfolio perspective fails to recognise the new approach to IT service alignment with corporate objectives advocated by ITIL v3 since 2007.<br>The process perspective does not describe the use of desirable practice and architecture. | This view of IT governance could complicate IT governance projects in the sense that it does not clearly spell out the roles, governance structures and enablers required for effective IT governance. | In applying the CPR Framework for IT governance, Costello and Laplante argue that sustained financial results must be the objective and the prime driver for IT governance. This is not coherent with most of the IT governance literature studied in this review, which requires IT to be aligned to the achievement of strategic organisational objectives regardless of whether they deal with financial results or other strategic aspects of the business.<br>The publication mentions a few IT processes and ITIL in passing, but overall, the proposed application of the CPR Framework provides a superficial IT governance model. | The model deals with IT governance in a superficial manner and provides inadequate guidance on roles, processes and clear mechanisms for successful IT governance.<br>The emphasis is almost exclusively on decision making and does not provide clarity on the question of who should make the decisions, how the decisions should be made and which questions need to be asked in the first place.<br>Furthermore, the paper deals more with understanding the extended enterprise than with IT governance itself. | The model could be improved by adding a more detailed narrative, especially related to the roles and structures.<br>The model includes aspects that are part of the normal corporate structure, including most of the compliance elements and vendor management, which is part of the greater supply chain management process.<br>In some aspects it is too light on detail, in others it includes items best left to the wider corporate structure. | The underlying perception is that IT governance is about decision-making structures.<br>This attempt to establish a framework for IT governance research over-simplifies the topic and offers little along the lines of a practicable IT governance framework or even the theoretical foundation for such a framework. |

**Table 2.2 – Comparative Summary of IT Governance Models**

## 2.8 Conclusion

As stated earlier, the requirements of King III and ISO/IEC38500 need to be incorporated into whatever IT governance framework this research proposes, in order to give it global (ISO) reach and local credibility (King III). Some 13 key implementation requirements were identified as prerequisites to such a proposed framework.

In terms of the six models compared in this chapter, the common, key elements required by the models include:

- Structures, including roles, bodies and stakeholders playing a role in administering the IT governance processes, and making decisions affecting IT and its use in the organisation. This includes the IT Steering Committee, programme management office, Office of the CIO and enterprise architecture function.
- Processes for IT governance, including the policies, procedures and standards used in implementing IT governance processes and structures. Specifically included in the collection of processes are IT risk management, compliance, performance management, portfolio management, strategic alignment and procurement.

The models considered in this chapter relate to the high-level IT governance model and therefore do not directly reference desirable practices or enablers. They are conceptual models and not at the practical, implementation-focused level of a comprehensive IT governance framework, that is, they focus on what needs to be done to achieve effective IT governance and do not incorporate the "how to" dimension required to implement the practical mechanisms underlying such effectiveness.

# Chapter Three: IT Governance Enablers

## 3.1 Abstract

The preceding chapter provided definitions of key terms used in this research, including the IT governance major processes. It went on to analyse six existing IT governance models. This chapter explores practices, standards and frameworks enabling IT governance.

## 3.2 Introduction

The Global Status Report on the Governance of Enterprise IT – 2011 (IT Governance Institute, 2011:29) listed the following practices, standards, and combinations of practices and standards as prevalent among the influences on global IT governance frameworks:

| Standard or Practice | Respondent Preference % |
|---|---|
| ITIL/ ISO/IEC20000 | 28% of respondents – an increase of 4% on the 2008 report |
| ISO/IEC17799/ ISO/IEC27000/ ISOTR13335/ ISF | 21.1% of respondents – more than double the 10% in 2008 |
| Six Sigma | 15.1% – up from 2% in 2008 |
| COBIT | 12.9% of respondents – 1.1% decrease on the 2008 report |
| PMI, PMBOK | 12.7% vs. 1% in 2008 |
| Risk IT | 12% |
| CMM/ CMMI | 9.3% of respondents vs. 4% in 2008 |
| ISO/IEC38500 | 8.2% |
| Prince2 | 6.4% – up from 2% in 2008 |
| ValIT | 4.9% – up from 1% in 2008 |
| TOGAF | 2.9% – slightly up from 1% in 2008 |
| COSO | 1.6% – slightly up from 1% in 2008 |

**Table 3.1 – Global Status Report on the Governance of Enterprise IT – Practices and Standards**

Some inferences may be drawn from the changes between the 2008 and 2011 reports, including the following:

ITIL has consistently remained the favourite IT governance tool and continues to gain support. ISO/IEC38500 and Risk IT, which were released since the 2008 report, rapidly gained popularity among the research group. Combined with the increased use of Val IT, this indicates a heightened awareness of and need for more specific guidance around specialised aspects of IT governance. The slight decrease in the popularity of COBIT is noted with interest. Considering the uncertainty around the use of COBIT 5, which was published since the 2011 Global Report, the researcher would not be surprised if this declines even further. It is also clear that information security (ISO/IEC27000) has climbed significantly on the priority ladder. Organisations seem to be looking for process improvements, as was indicated by the rise in adoption of Six Sigma. PMBOK and Prince2 adoption has increased notably, which shows a need for improved project governance.

In this section, each of the practices, standards, and combinations of practices and standards listed above is evaluated for inclusion in a proposed generic IT governance framework that was presented to the participants in this research for comment. In doing so, they considered the applicability and practicability of such a framework to their organisations. The research also considers which of the five IT governance major processes (Strategic Alignment, Value Delivery, Risk Management, Resource Management, Performance Measurement) are supported by the practice, standard or combinations.

## 3.3 ITIL

ITIL represents desirable practice for Service Management and the complete service lifecycle (Office of Government Commerce, 2007), from service strategy through to service operation, including all aspects of Service Support (Office of Government Commerce, 2000) and Service Delivery (Office of Government Commerce, 2000). Stenzel (2007:159) states that: “ITIL processes are a necessary component in IT’s maturity process”. The Global Status Report on the Governance of Enterprise IT – 2011 (Office of Government Commerce, 2011:29) shows that ITIL is considered the most referenced practice influencing IT governance frameworks.

ITIL has, for many years, been the only widely used IT service management framework. It supports the establishment of processes to preserve the operating integrity of the IT environment. The IT service management organisation represents the backbone of the live IT environment. Without the contribution made by ITIL over the years, the level of standardisation across organisations would not have been where it is today.

The ITIL 3 update introduced five complementary lifecycle titles (IT Governance Institute, 2009:20), covering the disciplines of service strategy, service design, service transition, service operation and continual service improvement. The ITIL 2011 is the latest update to ITIL 3. The Service Strategy (SS) module outlines the key processes of demand management, strategy generation, service portfolio management and IT financial management. SS covers strategic planning of IT service management capabilities, the alignment of IT service management capabilities to business strategy, guidance on value creation and the structure of services, with their providers. Service Design (SD) specifies the availability management, capacity management, continuity management, security management, service catalogue management, service level management, capacity and availability management, IT service continuity management, information security management, and supplier management processes as key to service design. SD addresses the design and development of services and supporting processes. Service Transition (ST) covers the processes of transition planning and support, change management, service asset and configuration management, release and deployment management, service validation and testing, and evaluation and knowledge management. ST shows how the requirements of SS and SD are realised and how capabilities for ongoing service delivery can be maintained. Service Operation (SO) deals with the effective and efficient delivery and support of event management, incident management, request fulfilment, problem management and access management. SO provides references to operational activities in other processes. Continual Service Improvement (CSI) covers ongoing service improvement and the measurement of process performance required for the service through service measurement, service reporting and service improvement.

The ITIL lifecycle modules cover IT from service strategy through its tactical and operational aspects. In an IT governance framework, it is essential to provide for a strong IT service organisation. ITIL provides this aspect.

In ITIL 2011, the former Service Support and Service Delivery publications were not replaced but incorporated into the Service Capability modules, namely: Planning, Protection and Optimisation; Service Offerings and Agreements; Release Control and Validation; and Operational Support and Analysis. Service Capability represents most aspects of operational IT processes and, as a set of practices, ITIL is of considerable importance as its processes map closely to most of the operational processes in COBIT 5. Forrester Research reported an increase from 13% to 20% of ITIL adoption by companies with revenue in excess of $1bn, while 90% of US companies have one or more IT service management projects underway (Conger, 2009:126).

### *3.3.1 Strengths and Limitations of Practice*

ITIL provides internationally accepted guidance for operational IT management, addresses all aspects of operational IT management, and provides strong guidance on operational IT processes. However, it does not spell out the process in detail and does not provide guidance on IT controls. Addy (2007:2-6) lists a number of arguments for and against the use of ITIL. Considering the scope of this thesis, some of the more relevant arguments for using ITIL include its structured approach, its provision of a common IT vocabulary, and its flexibility in terms of implementation options. On the negative side, Addy argues that "best" practice could be construed as average, and that too much structure could stifle creativity and the tendency of frameworks like ITIL to become "food for consultants". In terms of IT governance, companies have, over the years, often confused the needs fulfilled by COBIT and ITIL, propagating either ITIL or COBIT as a sufficiently comprehensive IT governance solution. COBIT and ITIL complement each other and should be used in combination (Stevens, 2011).

### 3.3.2 Impact on a Generic Framework

Bin Sahibuddin (2008:5) argues that ITIL 3 satisfies all aspects of a "well-matured IT governance framework", however, his paper fails to adequately explain how ITIL 3 rises above its operational focus to address all aspects of the IT governance major processes, even though it cites the IT Governance Institute's Board Briefing on IT Governance, where these processes are set out. This thinking was prevalent in the late 1990s and early 2000s, but the followers of ITIL and COBIT have since grown in their understanding of the position of the frameworks toward each other. In more recent publications, the understanding of the complementary roles these two frameworks play is described more accurately, for example, Costello (2006:311) explains ITIL as being an ideal complement to COBIT, where the former outlines IT process, while COBIT provides the control-level guidance. ITIL is no substitute for COBIT or vice versa.

COBIT should be combined with other prominent practices, standards and frameworks, such as ITIL for discrete process detail (IT Governance Institute, 2009:61). COBIT focuses on what should be addressed to ensure good governance of all IT processes. ITIL addresses how effective IT governance could be achieved for IT service management processes (IT Governance Institute[a], 2009:14).

As far as IT service management is concerned, several examples of ITIL-based service management frameworks exist, with the Microsoft Operations Framework (Microsoft, 2008), the HP Service Management Framework (Hewlett-Packard Development Company, 2007), and CA's Business Service Management Approach (CA, 2008) numbering among the more prominent examples. These frameworks were not intended to replace ITIL but rather represent it in the packaging of the particular vendor promoting his framework. As such, these frameworks did not pretend to be alternatives to ITIL but rather a customised "flavour".

The ITIL service lifecycle represents operational IT processes and, as a set of practices ITIL, is of considerable importance. During the research for this dissertation, no true alternative for ITIL could be found, only IT service management frameworks that are derivatives of ITIL. According to Betz (2007:36), the three major frameworks with the greatest effect on enterprise IT in the USA are COBIT, CMMI and ITIL.

ITIL has positioned itself as a pervasive framework touching all operational IT processes and the alignment of IT to organisational objectives. ITIL is a standard inclusion in publications citing "best" practices for IT governance. Calder (2006:21) describes ITIL as "a set of best practices at the heart of IT service management" and mentions that ITIL aligns with ISO/IEC17799 for information security management. Boonen (2007:9) also regards ITIL as best practice for service management. Kairab (2005:238) considers ITIL a service management best practice and a means of implementing security measures (the "how"), complementing ISO/IEC17799 (the "what"). In light of its complementary, operational role, it is understandable that participants in the Global Status Report on the Governance of Enterprise IT – 2011 indicated ITIL as the most referenced framework in the IT governance sphere. Its complementary stance towards COBIT 5 and ISO/IEC17799 means that organisations using these two frameworks could also be successful ITIL users.

## 3.4 ISO/IEC20000

ISO/IEC20000 is the ISO standard supporting certification of compliance with ITIL, covering both IT service management and information security management, the latter via a cross-reference with ISO/IEC17799 in Clause 6.6 (Calder, 2006:22). Organisations that require certification of the quality of their service provision use ISO/IEC20000 (BOONEN, 2007:10).

### *3.4.1 Strengths and Limitations of Practice*

Organisations that are standards-focused and require compliance certification find this a useful standard for evaluating compliance with ITIL IT service management and information security management practices. ISO/IEC is a global standard, which makes it useful for international benchmarking. As a standard, it focuses on compliance rather than the means of establishing an effective service lifecycle. Few organisations require formal certification of compliance with ITIL, which limits the usefulness of this standard.

### *3.4.2 Impact on a Generic Framework*

ISO/IEC20000 does not compete with ITIL as it measures compliance with various aspects of ITIL. As a global standard it is unique and has no alternatives, however, it is not suited for the generic IT governance framework proposed by this research, as the focus is not on certification but rather generally effective IT governance. ITIL is sufficient for governing the IT service management processes and practical aspects of the information security processes and ISO/IEC20000 compliance is therefore not a prerequisite for compliance with the proposed IT governance framework.

## 3.5 COBIT

The introduction of COBIT 5 saw the main publication, complemented by more specialist, focused publications, which at the time of this research included the Enabling Processes, COBIT 5 Implementation, COBIT 5 for Information Security, COBIT 5 for Assurance, COBIT 5 for Risk, and COBIT 5 Implementation. The researcher is a registered COBIT 5 Foundation trainer and regularly engages South African corporates on IT governance. From this interaction, limited appetite was observed for organisations making the transition to COBIT 5. The market is still digesting the flood of new COBIT 5 publications, debating their practicality and the maturity of the all new approaches COBIT 5 proposes. Even the auditing fraternity, which has always constituted the strongest support group, is not quite sure how to apply the new material. Despite this, the researcher expects a hybrid of COBIT 4.1 and COBIT 5 to continue to be a strong contributor to IT governance in South Africa and globally.

Considering COBIT's origins from among the audit community, it makes sense that there has traditionally been a strong relationship with IT assurance. Limited academic research exists that leverages COBIT, so there is still considerable opportunity for research in this field (Debreceny, De Haes, Van Grembergen, 2013). Interestingly, some recent research articles, for example Inaba (2013) and Debreceny (2013), still prefer to utilise COBIT 4.1. Al-Zwyalif (2013) did not even reference COBIT 5. Apart from the ISACA-related publications, few useful articles could be found on COBIT 5, which indicates limited availability of objective critiques of the new release. As ISACA owns COBIT, its critique of its own practice does not provide much value in assessing the fifth edition.

Using the COBIT 5 principles as a starting point, Forrester identified five strategic guidelines and practices for turning existing IT governance practices into business technology governance (Peters, 2012), namely: make business technology governance an integral part of business strategy; align cross-functional business processes; maintain an integrated framework; train staff and democratise decision making; and govern business technology from outside IT services provisioning. These are not new concepts and do not add much to the discussion on the interpretation of COBIT 5. COBIT 4.1 provided a comprehensive, internationally accepted set of IT control objectives, together with guidance on how IT processes map to the IT governance major processes, the roles and responsibilities within IT and IT process maturity. The 34 processes in COBIT 4.1 provided a structure for conceptualising the IT environment.

Having begun as a tool for auditors designed by auditors, the perception that COBIT is an audit tool still prevails among some (KAIRAB, 2005:234), although the release of COBIT 4 has assisted in changing perceptions, with more users realising the value of COBIT in establishing IT governance structures (Boonen, 2007:21). De Haes and Van Grembergen[a] (2009:1) found that there is a strong correlation between the implementation of COBIT and Val IT, and the achievement of IT goals.

Since its birth in 1996, COBIT has matured into COBIT 5 – at least that was the case at the time this research was undertaken. According to the Global Status Report on the Governance of Enterprise IT – 2011, it is the fourth most referenced among frameworks considered to be influencing IT governance and is unique as a commonly available, non proprietary practice. Betz (2007:36) ranks COBIT with ITIL and the Capability Maturity Model (CMMI) as among the top three "frameworks with the most effect on enterprise IT in the United States".

COBIT (IT Governance Institute, 2007) adopts a generic view of the IT environment, breaking it down into 34 processes that are grouped into the four domains of Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. Each of the 34 processes is broken down further into control objectives which are classified according to resource types impacted (applications, information, infrastructure or people), business requirements (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability), and IT governance major processes impacted. To facilitate formal process design, each process also has a suggested list of inputs from and outputs into other processes, a RACI chart summarising responsibilities and accountabilities for roles related to the process, goals and metrics, and suggested maturity ratings.

### *3.5.1 Strengths and Limitations of Practice*

COBIT bridges the gaps between business risk, control needs, and technical issues following an approach that supports the internal control environment (Fichadia, 2007:64). COBIT 4.1 provides the detailed IT control objectives to satisfy the requirements of the COSO framework (Moeller, 2008:144-145). The control objectives form the foundation for almost all possible IT controls. From an architectural point of view, COBIT provides an IT process model depicting IT processes, allowing a structured approach to building IT processes. The capability levels associated with each of the processes depicted by COBIT make it possible to monitor process capability and set maturity targets. COBIT is an international framework that is used by IT professionals, external auditors and internal auditors alike, providing a bridge that synchronises all parties' understanding of the control environment.

Despite the strengths listed above, application control guidance in COBIT 4.1 remained inadequate, with only six control objectives, AC1 to AC6 dedicated to application controls (IT Governance Institute, 2007:16). This was an area that was expected to improve in future releases. COBIT 3 attempted to cover application controls via process DS 11 – Manage Data, but this process was very mainframe-focused and became out of date, which necessitated an update. The update was, however, ineffective at addressing application controls.

Bloem (2006:236) states that the IT Governance Institute has positioned its COBIT framework as a de facto IT governance standard. What the IT Governance Institute failed to do in older publications was to contextualise COBIT vs. other IT governance frameworks. In more recent literature, such as the IT Control Objectives for Sarbanes-Oxley, 2nd Edition (IT Governance Institute[b], 2006) mention of ITIL and ISO/IEC17799 is made more often but the publications still do not always clearly explain how COBIT should be used in conjunction with other frameworks. COBIT provides a comprehensive set of IT control objectives but does not provide sufficient detail on the "how" of control design and implementation (Violino 2006:46).

### *3.5.2 Impact on a Generic Framework*

COBIT provides structure to the IT environment through the COBIT 5 process reference model and the COBIT 4.1 control objectives, with ITIL and other complementary practices providing guidance for establishing process detail. South African companies have invested years in IT governance structures and processes based on COBIT. COSO incorporates IT controls but, as it has an enterprise-wide focus, it does not provide sufficient detail to serve as an IT control framework in its own right. COBIT represents desirable practice for IT control objectives while COSO (2004) represents desirable practice for enterprise risk management, including the internal control environment. Moeller (2008:145) provides a mapping of the 34 COBIT 4.1 processes to the main components of COSO, which shows how COBIT addresses all aspects of the internal IT control environment COSO requires. The IT Governance Institute has published a similar mapping (IT Governance Institute, 2006:54).

At the 2013 ISACA and itSMFsa's SMEXA13 conferences, a number of discussions among delegates centred around the complementary use of COBIT 5 and ITIL. As previously explained, COBIT 4.1 specifically addressed IT controls and the high-level process architecture, but works best in combination with other frameworks and standards, such as ISO/IEC17799 and ITIL. As a set of control objectives and a high-level process architecture guide, no alternative that is generally available to companies and that would support a generic IT governance framework could be found during this research. From experience, the researcher is aware that some of the large international audit firms have control objectives and IT process maps, though these are proprietary and therefore do not lend themselves to supporting a generic framework.

As far as maturity guidance is concerned, the COBIT 4.1 maturity model was borrowed from CMMI, which could be considered an alternative for COBIT's process maturity measurement, however, it would not make sense to separate them, seeing that COBIT has assimilated the thinking and provides a ready-made set of maturity measures, based on CMMI. The COBIT 5 capability levels have since replaced the COBIT 4.1 maturity levels, though the adoption of the former is still slow. In the IT Governance Global Status Report – 2008 (IT Governance Institute, 2008), COBIT was the second most referenced practice and even though it has since dropped in the ranks, it still came within the top five practices in the 2011 report. COBIT provides an IT governance touch point among most of the frameworks and practices referenced in this dissertation, with the most prominent being ITIL and ISO/IEC17799.

As a non-proprietary, generally available framework of control objectives, COBIT 4.1 was unique. It assisted the chief enterprise architect in constructing a model of the IT environment, an area in which it is not unique, but provides common referencability among organisations and bridges the gap among auditors, business and IT management. COBIT 5 does not have a pronounced set of control objectives but its value in combination with COBIT 4.1 lies in its greater emphasis on process-level detail. For the purposes of this research and the draft discussion framework used as the basis for participant input, COBIT 4.1 is positioned as the desirable practice for control objectives. COBIT 5 still has to mature to a point where it is generally accepted and adopted by South African organisations before it will jutsify being positioned as part of a generic IT governance framework.

## 3.6 ISO/IEC17799, ISO/IEC20000, ISO/IEC13335

ISO/IEC17799 (ISO/IEC17799, 2005) provides guidelines and principles for initiating, implementing, maintaining and improving information security management (ISO, 2005:1). It includes a detailed set of information security control objectives and proposed controls, which need to be implemented to respond to relevant risks identified by a risk assessment. ISO/IEC17799 is based on part one of British Standard BS7799 (Fichadia, 2007:66). ISO/IEC17799 and ISO/IEC27001 have gained wide acceptance in the information security fraternity and should therefore be considered in the formulation of security-related policies, procedures and standards. ISO/IEC17799 provides "general guidance on the commonly accepted goals of information security management" (ISO/IEC17799, 2005:1). Compliance with ISO/IEC17799, which is a standard that covers information security in the broad sense, represents a mark of confidence in an organisation's overall security (Moeller, 2008:296-297).

The ISO/IEC27000 series currently includes ISO/IEC27001 (2005), which specifies the requirements for establishing an information security management system, and 27002, which has absorbed ISO/IEC17799 (Boonen, 2007:8). ISO/IEC27001 explains how ISO/IEC1779 (that is, ISO27002) should be applied (Moeller, 2008:299). In its third version, ITIL now provides guidance on the security management process as it relates to all other operational IT processes (Moeller, 2008:237). As such, ITIL V3 is an important complement to ISO/IEC17799 and ISO/IEC27001 for managing information security. The ITIL Information Security Management Process provides a security framework, information security policy and guidance for implementation of the ISO/IEC17799 security management system (Office of Government Commerce, 2007:142). ISO/IEC17799 and ISO/IEC27001 map back to COBIT process DS5 – Ensure Systems Security, which falls within the Deliver and Support domain.

ISO/IEC27000 references definitions and more detailed content in ISO/IEC13335. ISO/IEC TR 13335 Information Technology – Guidelines for the Management of IT Security is a technical report addressing aspects of IT security management, outlining IT security management tasks, the implementation and management of IT security, techniques for IT security management, control selection, and communication-related issues to be taken into account when introducing network security (IT Governance Institute [a], 2006:35).

### *3.6.1 Strengths and Limitations of Practice*

The ISO sets international benchmarks for information security under the ISO/IEC27000 series, which are widely known and understood. In organisations with high levels of process and IT governance maturity, ISO standards could prove invaluable for improving compliance to internationally desirable practices. In organisations of lower maturity, the implementation of ISO/IEC27000 could prove premature.

### *3.6.2 Impact on a Generic Framework*

COBIT process DS5 (Ensure Systems Security) provides high-level information security control objectives, while ITIL provides detail on the user administration process. The control objectives and model controls in the ISO/IEC27000 series are sophisticated and could prove more than smaller organisations or organisations with low process maturity are able to handle. Smaller organisations might find the user administration process in ITIL sufficient. In the context of this dissertation, which focuses on larger organisations, combinations of COBIT 5, ISO/IEC27000-based controls and ITIL-based user account management processes are relevant. Due to its sophistication, ISO/IEC27000 compliance was only presented as an option for organisations that have achieved at least a level 4 maturity for process DS5 in COBIT 4.1 (IT Governance Institute, 2007:120), which required the organisation to have the following: clearly assigned, managed and enforced IT security responsibilities; consistent performance of IT security risk assessments; formal IT security policies and procedures, with specific security baselines; standardised use identification, authentication and authorisation; security certification of security management and audit staff; formally implemented security testing processes and a related security improvement process; coordination of IT security with overall organisational security; IT security reporting to be linked to business objectives; IT security training to be conducted in both business and IT; and goals and metrics to be defined for security management.

## 3.7 CMMI

According to Bloem (2006:252), the Capability Maturity Model (CMM) is the best known and most widely used model for software process improvements. The Capability Maturity Model Integration (CMMI) succeeded the Capability Maturity Model (CMM) and focuses on developing and improving processes to meet business goals. In the IT context, the CMMI framework is often used for developing and assessing the software development maturity of organisations in the areas of process management, project management, engineering, and support (Betz, 2007:36).

### *3.7.1 Strengths and Limitations of Practice*

Betz (2007:36) listed CMMI alongside COBIT and ITIL as one of the most effect on enterprise IT in the USA. CMMI is internationally known, with maturity guidelines even built into the COBIT processes. The application of CMMI to monitor process maturity depends on the level of process formalisation and organisational maturity. In many organisations, processes have not been formalised and standardised to a level where process maturity could be measured successfully. The application of CMMI in this research will be limited to its use by COBIT as a generic guide on IT process maturity.

### *3.7.2 Impact on a Generic Framework*

The CMMI guidelines built into COBIT 4.1 ensured it was embedded in the proposed IT governance framework and was therefore initially regarded as an alternative to directly including CMMI in this research. The CMMI guidelines embedded into COBIT 4.1 assisted in the integration of frameworks, so CMMI was not included as a stand-alone framework but indirectly via the inclusion of COBIT 4.1. COBIT 5 has since departed from direct association with the CMMI, which is further justification for its omission.

## 3.8 Balanced Scorecard

In the early nineties, Robert Kaplan and David Norton coined the term, "balanced scorecard" (Kaplan, 1996:viii), a term that has since become widely used in corporate performance measurement circles. "The Balanced Scorecard provides executives with a comprehensive framework that translates a company's vision and strategy into a coherent set of performance measures (Kaplan 1996:24)." The Balanced Scorecard is "a carefully selected set of quantifiable measures derived from an organisation's strategy" (Niven, 2006:13). Many variants of the original balanced scorecard exist but are all based on the initial concepts Norton and Kaplan articulated (Olve, 2006:15). The balanced scorecard provides an effective framework for implementing governance communications, based on its focus on strategic alignment, its perspective beyond financial measures, and its combination of leading and lagging metrics (Symonds, 2009:4). Epstein (2005:41) states that an effective IT balanced scorecard could benefit the organisation by demonstrating IT's contribution to organisational success, assisting IT managers in prioritising projects according to their value to the organisation, aligning the IT strategy to organisational objectives and providing a measure of actual IT performance against plan. Some organisations go further and apply the balanced scorecard concept to measuring return on investment (Borck, 2001:54).

### *3.8.1 Strengths and Limitations of Practice*

The balanced scorecard is an internationally known, accepted and implemented mechanism. It requires an organisation with clear strategic objectives, mature management and strong implementation mechanisms, for example a PMO to drive and report against implementation programmes. Not all organisations have these elements in place, which makes it difficult to apply the balanced scorecard in some environments.

### *3.8.2 Justification for Inclusion or Omission from Generic Framework*

There are many performance measurement and management tools available of which the balanced scorecard is one of the better-know alternatives. The emphasis is on performance measurement rather than any one mechanism for achieving that. Inclusion of the balanced scorecard is not a prerequisite to fulfilling the requirements of the generic IT governance framework; rather practicing an effective means of performance management is.

## 3.9 Six Sigma

Six Sigma aims to improve business processes to virtually error-free performance through a rigorous, focused implementation of proven quality principles and techniques (Pyzdek, 2003:3). Where a traditional company accepts a sigma three to four performance level, Six Sigma requires an almost zero process defect rate, that is, only 3.4 per one million opportunities (Bruce, 2005:ix), which many organisations cannot afford. Six Sigma is a philosophy that requires support from managers at all levels to succeed (Bruce, 2005:ix).

### 3.9.1 Strengths and Limitations of Practice

Six Sigma is an internationally known, accepted and implemented mechanism for process improvement. Many success stories exist to attest to its effectiveness in reducing process defects, however, it is an organisational mechanism rather than one specific to IT or IT governance. Six Sigma sometimes requires staff to be removed from their normal duties and be dedicated to Six Sigma teams focusing on problem resolution. In some organisations this may not be feasible. Six Sigma team members also need to be certified for their roles, which is both costly and time consuming. The following question should be raised: how many organisations really need to strive to zero defect processes?

### 3.9.2 Justification for Inclusion or Omission from Generic Framework

Many process and quality improvement methods and techniques exist. Six Sigma is a popular and perhaps better-known option in this field. As far as IT governance is concerned, process improvement through Six Sigma would not be a prerequisite. Performing IT process assessments against the CMMI process maturity guidelines in COBIT and initiating projects to raise IT process maturity levels to the organisation's target levels would be adequate for the purposes of the generic IT governance model.

## 3.10 Prince2

Prince2 provides a structured method for effective project management (Office of Government Commerce, 2009), whereas PMBOK is the definitive work on project management standards. As such, it complements PMBOK, providing the "how", while PMBOK states the "what". The current edition of Prince2 was released in 2009. Prince2 defines a project management method, providing a framework for the wide variety of project disciplines and activities. Prince2 focuses on the business case, which drives all project management processes from initiation to conclusion (IT Governance Institute [a], 2006:46). Considering the findings of the Global Status Report on the Governance of Enterprise IT – 2011, PMBOK and Prince2 are considered project management-related desirable practice and have both grown considerably in popularity as PMOs become more structured and formalised. A Mapping of Prince2 with COBIT 4.0 (IT Governance Institute [a] 2007:22) shows that Prince2 directly maps to and supports the COBIT 4.1 process PO10 – Manage Projects. For completeness, also refer to the programme management office paragraph of the IT governance structures section.

### *3.10.1 Strengths and Limitations of Practice*

Prince2 is an internationally known, accepted and implemented project management method, with a large number of international practitioners certified through the ISEB examination board. Furthermore, it provides a generic approach to project management that is suited to any type of organisation. Prince2 does not address programme or project portfolio management. For the purposes of this research, the emphasis will be on minimal requirements for IT governance, for which project management is sufficient. A point of criticism that is sometimes levelled at Prince2 is the emphasis on documentation. A lesser experienced project manager could potentially fall into the trap of spending too much time on documentation, at the expense of project delivery.

### *3.10.2 Justification for Inclusion or Omission from Generic Framework*

There are several proprietary project management methodologies that satisfy the requirements of PMBOK and could be used successfully instead of Prince2. PMBOK should not be considered an alternative to Prince2, as the former provides the project management standards, while the latter addresses methodology. Unlike a proprietary project management method, Prince2 has global reach, but any method satisfying PMBOK would be acceptable in terms of the framework. Prince2 could be used in conjunction with other PMBOK-friendly methods.

## 3.11 COSO

The Securities Exchange Commission in the United States of America (US SEC) recommends the COSO enterprise risk management integrated framework (COSO, 2004) as the internal control framework for compliance with the Sarbanes-Oxley Act (IT Governance Institute$^{b}$, 2006:55). COSO incorporates IT controls but, as it has a wide enterprise focus, it does not provide sufficient detail to serve as an IT control framework in its own right. COSO (2004) represents desirable practice for enterprise risk management, including the internal control environment. Moeller (2008:145) provides a mapping of the 34 COBIT processes to the main components of COSO, which shows how COBIT addresses all aspects of the internal IT control environment COSO requires. The IT Governance Institute (2006:54) published a similar mapping. COSO is referenced as the international baseline for internal control systems, being the most comprehensive study on internal control. It enables management to establish internal controls in support of the achievement of organisational goals. COSO focuses on the overall organisational control environment and, while it does not reference IT specifically, its control principles apply equally to the IT control environment (IT Governance Institute$^{b}$, 2006:16-17).

### *3.11.1 Strengths and Limitations of Practice*

COSO is the internationally known and accepted standard internal control framework. It does not directly address internal IT controls and therefore needs to be combined with COBIT to realise its value for IT governance.

### *3.11.2 Impact on a Generic Framework*

As a high-level internal control framework COSO has no real alternative. The US SEC, together with the IT Governance Institute's publications on IT governance, reference it as the internal control framework against which COBIT is applied. COSO will not be included directly in the generic framework as it does not directly address IT governance. COBIT is, however, aligned to COSO and will be included.

## 3.12 PMBOK

PMBOK, published by the Project Management Institute, is the definitive work on project management standards and provides general guidance on all aspects of project management. The IT Governance Institute suggests the use of PMBOK as a source of detail for the IT project management process, as COBIT only provides high-level detail (COBIT process PO10), in the form of control objectives for the process (IT Governance Institute, 2004:7).

PBMOK is an American National Standard (ANSI/PMI 99-001-2004) described as the sum of knowledge of the project management profession (IT Governance Institute, 2004:18). Today, PMBOK is the de facto standard for project management (Dvir, 2007:9). According to the Global Status Report on the Governance of Enterprise IT – 2011, PMBOK and Prince2 are considered project management-related desirable practice. According to the PMBOK Guide (Project Management Institute, 2004), for a project to be successful the project team must select appropriate processes to meet project objectives, use a defined approach for adapting project specifications and plans to meet project and product specifications, comply with requirements to meet stakeholder needs, wants and expectations, and balance the competing demands of scope, cost, time, resources, quality and risk to produce a quality product.

PMBOK provides a detailed standard for all aspects of project management, including integration, scope, time, cost, quality, human resources, communication, risk and procurement management. Prince2 provides a structured method for effective project management (Office of Government Commerce, 2005:1), that is, meeting the standard defined by PMBOK.

For completeness, also refer to the programme management office paragraph of the IT governance structures section.

### *3.12.1 Strengths and Limitations of Practice*

PMBOK is an internationally known, accepted and implemented reference work that is open to many comprehensive, modern project management methods. PMBOK is a comprehensive and in some sense overwhelming set of requirements. Without a specific method like Prince2, implementing PMBOK is a daunting task.

### *3.12.2 Justification for Inclusion or Omission from Generic Framework*

As PMBOK is the de facto standard, there is no clear alternative to it. Many project management methods, for example Prince2, derived from PMBOK, complement it, but do not represent an alternative. No alternative to PMBOK could be found as far as project management standards are concerned.

## 3.13 TOGAF

The Open Group Architecture Framework (TOGAF) provides a generic enterprise architectural framework to a wide community in a similar way the Open Source Movement supports sharing of software. The international trend is for most organisations not to have a formal enterprise architecture (EA) function or even formal sub components, including business, infrastructural, data or information architecture (Scott, 2008:2), which indicate that EA is still a young and evolving function. Internationally, EA team size and structure vary greatly (Scott, 2008:10). In its list of frameworks influencing IT governance, the IT Governance Global Status Report – 2008 (IT Governance Institute, 2008:36) only included TOGAF as an architecture framework. Even though it was not referenced by that many organisations, it still made the list. In the 2011 report this remained the case. The Global Status Report on the Governance of Enterprise IT – 2011 (IT Governance Institute, 2011:23) cited Prince2 and TOGAF as the most popular IT-related certifications, which further supports inclusion of these two practices in a generic framework.

With the increasing number of publications such as ITIL advocating a services orientation, organisations might do well to consider the suitability of adopting a service-oriented architecture, which makes services available in a transparent manner (Baschab, 2007:307). TOGAF supports SOA (Capgemini 2008:248) and may therefore be worth considering if an organisation embarks on the enterprise architecture journey, with a view of transforming to a service-oriented architecture. Enterprise architecture aspects, as far as the roles of the chief enterprise architect and Enterprise Architecture Forum are concerned, are discussed in the IT governance structures section.

### *3.13.1 Strengths and Limitations of Practice*

TOGAF is an international framework that is shared by a large community of certified practitioners. The role played by the consulting firm Capgemini to rewrite and modernise TOGAF has contributed to the quality of the framework but could be construed as a point of contention in the framework's challenge to be "open" rather than quasi proprietary. The framework has undergone several development iterations and some might argue that it has not yet stabilised to a level where it could be regarded as the definitive standard for enterprise architecture. This field is still developing, so a combination of tools may be required for the foreseeable future.

### 3.13.2 Justification for Inclusion or Omission from Generic Framework

Weill and Ross have written several publications on enterprise architecture and, as individuals, have contributed much to the thinking around EA. TOGAF is gaining ground, though few organisations have reached a point where their EA is stable enough to standardise on a single framework. Most use a combination of EA tools and frameworks. The generic framework will not insist upon the inclusion of TOGAF or advise against it. Organisations would instead be encouraged to study TOGAF together with other EA frameworks and find a combination suitable to their needs.

## 3.14 VALIT

The ValIT Framework, originally published by the IT Governance Institute during 2006, provides a useful structure for value delivery, comprising value governance, portfolio management and investment management. It supports the realisation of optimal value from IT investments at an affordable cost, with an acceptable level of risk (IT Governance Institute, 2008). COBIT 5 now includes ValIT.

### 3.14.1 Strengths and Limitations of Practice

ValIT is a unique publication in IT. With all the effort devoted to its development, this framework is already in its second release. The precedent which COBIT set appears to be a positive indicator that the IT Governance Institute might have similar success with ValIT. The framework is still developing and needs to be promoted more widely before it will gain greater acceptance.

### 3.14.2 Justification for Inclusion or Omission from Generic Framework

During this research no formal, widely available alternatives for this publication could be found. At this stage, ValIT would not be included in the framework due to its current level of maturity and the lack of evidence of implementation by South African companies.

## 3.15 SysTrust

SysTrust comprises a set of assurance and advisory services based on a common framework to evaluate the reliability of information systems. It was develop by the American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants and only accountants qualified through these two bodies are allowed to perform a SysTrust audit (Kairab, 2005:240). Very little reference to SysTrust could be found during the literature review for this research.

### 3.15.1 Strengths and Limitations of Practice

When developed, SysTrust was regarded as a significant step towards establishing an effective continuous auditing infrastructure (McPhie, 2000:7). SysTrust provides a common standard for IT assurance and advisory services but due to the geographic restrictions (to North America) on its use it is not a feasible option for the South African organisations included in the research for this dissertation. SysTrust is also a tool for auditors to apply during their audits. As the scope of this research adopts the perspective of the CIO and his or her team, SysTrust is not regarded as relevant.

### *3.15.2 Impact on a Generic Framework*

SysTrust is not relevant to this research, as it is purely an auditor's tool. The scope of this research does not require an auditor's perspective.

## 3.16 IT Sub Processes

The IT governance major processes provide the five broad process classes, which require IT sub-processes within each class. For an effective internal control environment that supports corporate governance, information technology controls need to mature to a level where they could be relied upon to preserve the confidentiality, integrity and availability of information assets. As a prerequisite to an effective system of internal IT control, however, it is necessary to raise IT sub-process maturity to a level where controls could be embedded firmly in the process. Low process maturity complicates control over processes and could increase the cost of implementing controls. Control design is driven by risk assessments and is captured in an IT control framework, which is translated into policies, procedures, standards and methodologies to implement the required governance mechanisms. Enabling components are broken down into policies, procedures, standards, methodologies, and risk assessments.

COBIT 4.1 (IT Governance Institute, 2007) incorporates process maturity classifications and metrics into the COBIT framework for their use during process formalisation and improvement initiatives. It represents a desirable practice for IT control objectives and a common point of reference for IT professionals and auditors alike. A study of 51 organisations from North America, Europe and Asia found that security and anti-virus management, management of the physical environment and IT financial management were typically the most mature processes. The least mature IT processes were IT performance monitoring, architecture and value management (Debreceny, Gray, 2013).

## 3.17 IT Control Framework

The IT internal control component represents a significant portion of IT governance. As part of the proposed IT governance framework, IT controls should be formalised in an IT control framework, based on the COBIT control objectives and other relevant control objectives, for example, those contained in ISO/IEC27000, for information security.

## 3.18 Supporting Documents

The documents "legislating" IT governance in the organisation include policies, standards, procedures and risk assessments. These documents provide the substance behind the processes and control framework in an IT governance framework.

### 3.18.1 Policies

IT policies lay down the principles that influence and guide the execution of IT procedures and the application of IT standards in line with the philosophy, objectives and strategic plans established by the Office of the CIO. IT policies also describe the consequences of non-compliance with the principles they define. Good policies meet the following criteria (Le Veque, 2006:131): assignment of enforcement responsibilities, accompanied by enforcement mechanisms; definition and allocation of roles and responsibilities; and clarity on desirable vs. non desirable behaviour. Being the owner of these documents, the CIO is accountable for the maintenance and overall enforcement of all IT policies and standards across the organisation. Standards and procedures offer a clearer method for implementing policies, which are high-level documents by nature (Peltier, 2004:48).

### 3.18.2 Standards

The mandatory requirements of individual policies are set out in standards (Peltier, 2004:49). Standards describe the desirable outcome of processes (Le Veque, 2006:131) and sometimes the minimum configuration requirements for specific technologies, or the minimum performance requirements for specific actions, in support of policies and procedures.

### 3.18.3 Procedures

Peltier (2004:50) describes procedures as, “mandatory, step-by-step, detailed actions required to successfully complete a task”. Procedures describe process flows, that is, the approved steps involved in executing IT processes (Le Veque, 2006:131). These procedures belong to the heads of the various IT departments, who are responsible for the customisation, implementation and maintenance of IT procedures for their individual departments.

### 3.18.4 Risk Assessments

Risk assessments involve management identifying and analysing relevant risks that could prevent IT from achieving its objectives, as a basis for the design of controls making up the IT control framework (IT Governance Institute [a], 2006:23).

## 3.19 Architecture

Enterprise architecture is an important mechanism for integrating IT and the business (M2PressWIRE, 2009). Architecture is covered under the TOGAF sub paragraph (2.2.1.11) and the role of the chief enterprise architect in 2.3.1.3.3. Being an important mechanism for IT governance, organisations continue to explore this area and the available supporting tools. In its current evolutionary phase, the value derived varies from organisation to organisation, with the Gartner Group having previously predicted that 40% of enterprise architecture projects are likely to be stopped (Saran, 2007:18). In light of the extensive coverage of architecture under the TOGAF, Chief Enterprise Architecture and Enterprise Architecture Forum paragraphs, this section has been limited to the above.

## 3.20 Portfolio Management

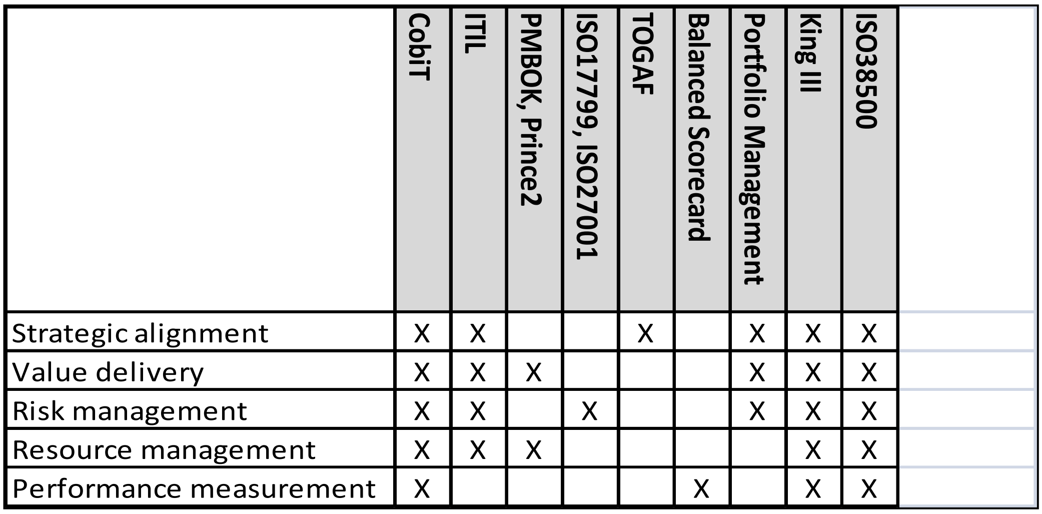
Addressing the challenges related to strategic alignment in an IT governance framework requires several mechanisms. One such important mechanism is portfolio management, with an IT portfolio as a sub set thereof. Portfolio management ensures the justification of investment in terms of strategic organisational objectives.

The 2010 CHAOS Manifesto (Standish Group, 2011) showed that only 37% of all projects truly succeed in terms of being delivered on time, on budget, and with the expected features and functionality. A further 42% of projects are delivered, yet are late, over budget or below expectation. Some 21% of all projects fail outright. Portfolio management is concerned with executing the strategic direction set for investments, including evaluating, prioritising and balancing programmes and services (ISACA[a], 2012). It further manages demand within resourcing and financial constraints, based on alignment with strategic objectives, enterprise value and risk. Portfolio management optimises portfolios by including and excluding projects and programmes as priorities change, and monitors portfolio performance on a continual basis.

A portfolio could comprise multiple programmes or projects, or even just the projects within a single programme (Brown, 2008:195). Portfolio management is a developing area which authors view in a number of different ways. Handler (2005:107) identifies three IT phases, with three corresponding areas of IT portfolio management, including: IT discovery portfolio management, which comprises potential growth and transformative IT investments in innovative and emerging technology; IT project portfolio management, which focuses on expanding replacing or fixing IT solutions; and IT asset portfolio management, which covers the IT infrastructural, application, human resource, information, data and process assets invested in maintaining, redeveloping or repositioning IT assets. The ValIT Framework (IT Governance Institute, 2008) provides a useful structure for value delivery and covers portfolio management as one of its three focal areas. It has since been incorporated into COBIT 5. As part of its extension, ITIL V3 has added service portfolio management, which aligns IT services to business (Office of Government Commerce, 2007:119). Project portfolio management manages the process of translating strategy and objectives into the appropriate project, before focusing on the execution of these projects. A recent public sector study indicated an improvement in overall project success of 30 to 40% from implementing PPM (EY[a], 2013:33-34). Norton and Kaplan (2004:13) propose strategic IT portfolio management as one of three approaches to align intangible assets to organisational strategy, by aliging the strategic IT portfolio to information capital.

## 3.21 Mapping of Practices and Standards to IT Governance Major Process

This section explores which desirable practices to include in a proposed, generic IT governance framework. Those practices that were recommended or the use of which has been encouraged, are listed in Table 3.2 below, with a mapping to each of the IT governance major processes each supports:



| | CobiT | ITIL | PMBOK, Prince2 | ISO17799, ISO27001 | TOGAF | Balanced Scorecard | Portfolio Management | King III | ISO38500 |
|---|---|---|---|---|---|---|---|---|---|
| Strategic alignment | X | X | | | X | | X | X | X |
| Value delivery | X | X | X | | | | X | X | X |
| Risk management | X | X | | X | | | X | X | X |
| Resource management | X | X | X | | | | | X | X |
| Performance measurement | X | | | | | X | | X | X |

**Table 3.1 – Desirable Practice Mapping to IT Governance Major Processes**

Table 3.1 indicates that COBIT is the most versatile IT governance practice, mapping to all IT process areas. As a more operationally focused framework, ITIL makes an important contribution towards implementing the process aspects of IT governance. Through their contribution to project and programme management, PMBOK and Prince2 contribute to value management (as a sub set of value delivery) and the management of project resources. The security aspects of IT risk management are primarily addressed by ISO/IEC27001 (ISO/IEC17799 is mentioned from a historic perspective), while TOGAF supports enterprise architecture as a strategic alignment tool. The balanced scorecard as described by Norton and Kaplan represents the primary performance management (including measurement) tool across the organisation, including IT. Portfolio management is not supported by any specific practices but contributes greatly to the alignment of IT programmes to organisation objectives, monitoring the value generated by programmes, and programme and project risk management.

As versatile, over-arching IT governance guidelines, ISO/IEC38500 and King III have been welcome additions to the IT governance body of knowledge. Significant developments in the field of IT governance in recent years, including the introduction of COBIT 5, a comprehensive update to ITIL, the publication of the King III report, with its emphasis on IT governance and the first international standards on IT governance (ISO/IEC38500), have presented more concrete material to work from than was previously been available in the field.

## 3.22 Conclusion

Several processes and standards are available to enable the desireable practices required for effective IT governance. These practices support the five IT governance major processes by providing the detail required to implement the detailed sub-processes. A summary of the practices discussed in this chapter, along with the IT governance major processes they support, has been provided in Table 3.2.

# Chapter Four: IT Governance Structures

## 4.1 Abstract

Chapter three presented practices, standards and frameworks that enable IT governance. Chapter four focuses on the structures and roles that are accountable and responsible for IT governance.

## 4.2 Introduction

Effective IT governance requires clear roles and responsibilities, especially the role played by executive management. The CEO is responsible for executing strategy and as such depends on the CIO to support this through IT (De Haes, Van Grembergen[a], 2008:26). For this research, the IT governance structures regarded as most significant are discussed below and include the office of the CIO, with its main sub roles; the IT steering committee, which focuses on tracking IT investment, setting priorities for IT and allocating scarce IT resources; the IT Strategy Committee, which concerns itself with IT/business alignment, balancing IT investment in current vs. future organisational needs, and specific IT enablement requirements for new directions in business; the enterprise architecture forum, which focuses on the structural composition of IT and its context within the wider organisation; and the PMO, which oversees the execution of programmes and projects in fulfilment of the strategic objectives of IT, as a sub set of the wider portfolio of projects in the organisation.

It has been found that it is easier to implement IT governance structures than to implement IT governance processes (De Haes, Van Grembergen[b], 2009). Relational mechanisms, which facilitate active participation and collaborative relationships among executives, IT management and business line management, are very important in the beginning stages of an IT governance project, though they become less important once the IT governance framework is embedded into the organisation's operations.

## 4.3 Office of the CIO

This section covers the main responsibilities of the CIO, differentiates the role of CIO from that of CTO (Chief Technology Officer), and briefly explains what other roles report directly into the Office of the CIO.

Unlike the role of a Chief Executive Officer (CEO) or Chief Financial Officer (CFO), the role of CIO could vary significantly from organisation to organisation. The objective of this section is not to dictate the establishment of a formal Office of the CIO but rather to summarise the roles and responsibilities related to the management of IT. By adopting the term, "Office of the CIO", the extent of the CIO's management team is clearly identified and the management roles clearly spelt out.

It is important to note that the roles mentioned in this section do not necessarily equate to positions, that is, some of these roles could be combined into a position, provided that such a combination does not go against the principle of segregation of duties. Ross (2009:105) refers to this team as the "IT leadership team". The emphasis here is not on the name of the body but rather on the principle that such a team should exist. A particular challenge faced in this section is the lack of generally accepted definitions of the roles of CIO and CTO, and of clear differentiation between the two roles, which are often combined into one.

This literature review does not favour a particular structure of the IT function, as that would depend on the nature of the organisations involved in the research for this dissertation. The purpose of the paper is to arrive at an IT governance framework that would suit any of the large organisations involved in this research, regardless of whether they had a centralised, federated or combined IT structure. All of these combinations are represented in the group of CIOs selected to participate in the research, so the framework should be effective regardless of the structure.

### 4.3.1 Duties of the CIO

Over the past two decades, the role of the CIO has largely focused on deploying IT and controlling costs (Bottger, 2008:218-219), however, the CIO's role should be one that is business oriented, rather than a technically oriented role in order to act as a bridge between IT and the rest of the organisation (IT Governance Institute, 2003:15). In 2003, the IT Governance Institute described the CIO's main responsibilities (IT Governance Institute, 2003:51) as IT-centric activities, including IT strategy, securing resources, establishing IT project management principles and thought leadership on the value of IT.

In more recent years, IT thought leaders such as Rangaswami started arguing that the role of the CIO could disappear in the near future (Riley, 2005:10). In fact, Rangaswami predicted in 2005 that the role of CIO would disappear within 10 years. Cranfield Business School and Deloitte made a similar claim in 2008, reiterating the idea, albeit according to a slightly longer timeframe (Ashford, 2008:7). Others, like Mahoney (2008), emphasise the changing role of the CIO, moving ever closer to the business and further away from technology, eventually being subsumed in business. The growing consensus seems to be that the CIO role is changing, which implies that organisations need to monitor these developments and adapt the role of IT leadership. Considering the changes in the international business world in recent years, CIOs are now expected to excel at more effective IT/business alignment and find ways of driving improved operating models, cost structures and long-term competitiveness through IT innovation (Chui, Edin, Manyika, 2009:4-5).

EY (2012) research shows that 17% of CIOs are members of the executive committee, although 48% of the C-suite (top-level executives) do not think the CIO is involved in discussing business performance and challenges. The C-suite's typical expectations of the CIO include operational basics, tight security, technology consultancy, change leadership, and the flexibility to move with shifting business needs. It also became apparent that businesses have low expectations of IT in terms of challenging the C-suite.

In what is being called the "new normal", CIOs are not only expected to have extensive IT experience but also demonstrate an understanding of business and industry. It is common to find CIOs with less than two years' experience in their organisations, due in part to their need to show quick, visible results and in part to the high demand for successful CIOs. A substantial component of current CIOs have come through the ranks of their companies, often via the head of applications development role. Where CIOs are expected to play a more strategic role they sometimes report directly to the CEO (Brown, Van Metre, 2008:2-3).

### *4.3.2 Justification for Role*

Mahoney (2008:3) predicted that by 2012 at least half of top-performing business will cite their IT contribution in the top three success factors. With IT playing an increasingly important role, it stands to reason that its leadership role is of great importance to the organisation, regardless of what it is called or where it is positioned in the organisation.

### *4.3.3 Potential Role Combinations*

Many organisations do not differentiate between the roles of CIO and CTO, and no single, globally accepted definition exists for either of these roles, so it is possible to combine the CIO and CTO roles into one position.

## 4.4 Chief Technology Officer

The CTO considers the appropriateness of technology acquisitions in view of the IT and organisational strategies, focusing on effectiveness (doing the right things) and efficiency (doing things right) (Bottger, 2008:202). In an organisation where the CTO assumes a technical, engineering role, this role might reside outside the IT department.

### *4.4.1 Justification for Role*

The CTO role is justified on an organisation-by-organisation basis, depending on the needs and culture of the organisation. It is not a standard role to be found in all IT environments.

### *4.4.2 Potential Role Combinations*

Some organisations combine the CIO and CTO roles, although in a highly technical engineering or telecommunications environment that might not be possible.

## 4.5 Roles within Office of the CIO

This section considers four roles traditionally associated within the office of the CIOs, namely the information security officer, chief enterprise architect, IT financial manager and IT risk officer. These are not necessarily full-time positions but areas of responsibilities that are assigned by the

Office of the CIO. New roles being defined for the Office of the CIO include those of the IT planning manager, IT PMO office manager and IT vendor manager.

The IT planning manager is responsible for the creation and maintenance of IT planning, communication of business needs to IT and education of stakeholders in business on what the IT organisation can do for the business (Cecere, 2009:1). The IT PMO manager is responsible for the effective delivery of the portfolio of IT projects and, by implication for IT project governance, maintaining project management standards, and project monitoring and reporting (Cecere, 2009:2-3). The IT vendor manager is responsible for managing IT suppliers and the relationship with them, collaborating with business and IT to set sourcing strategies and define vendor oversight processes. This roles requires a procurement expert responsible for monitoring IT vendor viability, especially as far as security and disaster recovery are concerned (Cecere, 2009:5). As these three roles have not yet matured and become general practice in IT organisations, they are not included as generic roles in a generic IT governance framework.

### 4.5.1 Information Security Officer (ISO)

The ISO is responsible for formulating information security policies, procedures and standards aligned to international standards and practice, for example ISO/IEC27000, and for monitoring compliance with approved security policies, procedures and standards. Although no de facto standard for the role of information security manager exists (ISACA, 2008:5), ISACA identifies five job practice areas for ISOs, namely information security governance, risk management, information security programme development, information security programme management, and incident management and response (ISACA, 2008:10-13).

#### *4.5.1.1 Justification for Role*

Information security management represents a key area of IT governance, to the extent that some people even wrongly believe it to be the only important area on this topic. It requires a significant level of skill and expertise, which is often not found in other roles.

#### *4.5.1.2 Potential Role Combinations*

Due to the requirement to segregate the role of ISO from operational roles, it is difficult to combine it with other IT roles. It does, however, combine well with operational risk management roles.

### 4.5.2 Chief Enterprise Architect

The enterprise architecture consists of four parts, namely the business, information, application and technical architecture layers (Baschab, Piot, 2007:300). The enterprise architecture represents the organising logic for business process and IT infrastructure and reflects the integration and standardisation requirements of the company's operating model. It provides a long-term view of a company's processes, systems and technologies so that individual projects can build capabilities (Robertson, Ross, Weill, 2006:8).

The chief enterprise architect segregates the enterprise architecture layers and outlines the architecture of each layer, formulates architectural standards and monitors compliance with these standards. The Enterprise Architecture Forum oversees the definition of architectural standards (IT Governance Institute, 2003:52), alignment of the IT organisation with organisational objectives and the maintenance of architectural integrity, and instituting action against parties that do not comply with architectural standards.

The chief enterprise architect focuses on the alignment of corporate strategy to the processes and systems of the enterprise (Handler, 2009:1). The chief enterprise architect also facilitates and encourages compliance with standards for the organisation, considering both strategy and project execution (Cecere, 2009:5). In some organisations, the chief enterprise architect reports into a business portfolio, sometimes even the CEO, though this role generally reports directly to the CIO (Handler, 2009:6).

This literature review identifies the chief enterprise architect as important to the effectiveness of IT. As shown in the Enablers section, enterprise architecture is still a young, evolving function. For this reason it is not possible to determine the optimal reporting line, that is, whether the chief enterprise architect should report into the Office of the CIO or into another business function like corporate strategy. Considering the fact that current awareness of this role is strongest in IT in most organisations, the role in its current form would probably be retained in IT, which is the position adopted by this research. Regardless of the choice of reporting line, a principle that should be adhered to is that the IT architecture role cannot be outsourced (White, 2001:292).

#### *4.5.2.1 Justification for Role*

Mahoney (2008:3) predicts that future decisions about IT will increasingly focus on architecture and exploitation of information, processes and relationships, rather than technology. That correlates with Gartner predictions about CIO roles becoming more business and less technology focused. Although this dissertation has shown that enterprise architecture is relatively immature in most organisations, it is a growing field and an absolute necessity for the long term.

#### *4.5.2.2 Potential Role Combinations*

The changing role of the CIO might in future lend itself to a combination with aspects of the enterprise architect role, but in the short to medium term this role will possibly share resources across the IT function or rely on external consultants rather than always being a dedicated internal role.

### 4.5.3 IT Financial Manager

IT financial management is a role that could justify a full-time position in many large IT organisations, but it could also be an allocated responsibility, rather than a position (Office of Government Commerce, 2001). The IT financial manager oversees the capital and operational IT budgeting process and monitors actual vs. budgeted IT expenditure, as well as IT programme spend at a portfolio level. Depending on the maturity of the organisation, the IT financial manager costs IT services per the service catalogue to the various end-user departments, and, if required by policy, charges these costs back to the individual departments. He or she is also responsible for monitoring compliance of IT procurement with organisational policies and procedures, and with IT hardware, software and service standards.

#### *4.5.3.1 Justification for Role*

ITIL strongly promotes the IT financial management role but not necessarily a full-time position. In large environments, however, a full-time position is often justified.

#### *4.5.3.2 Potential Role Combinations*

This role could be combined with other senior roles in IT, provided the person assuming it has the necessary financial management skills.

### 4.5.4 IT Risk Officer

Many publications exist on Enterprise Risk Management (ERM) and its direct sub processes, yet few comprehensive works have been published on the IT Risk Management specialisation, apart from the recently published Risk IT exposure draft (IT Governance Institute, 2009). Risk IT defines the IT risk management process model in three domains, namely risk governance, risk vvaluation and risk response. It assigns accountability for IT risk management to the chief risk officer, and makes provision for the creation of an IT risk officer role.

#### *4.5.4.1 Justification for Role*

ERM incorporates operational risk management, which in turn could be responsible for the IT risk officer role. Again, this is a role rather than a position.

#### *4.5.4.2 Potential Role Combinations*

The role of IT risk officer could be combined with an operational risk management role outside IT. The benefit of this would be that the officer would then be truly independent of IT. It should, however, be noted that both ERM and IT risk management are maturing fields, so there would be no single, best structure. It depends on the organisation.

### 4.5.5 Applications Manager

The applications manager is responsible for managing applications through their lifecycle. He or she could play a significant role in systems development, although that is not a prerequisite. The applications manager is the custodian of technical application management knowledge and expertise and provides the balance between the cost and skills level of application management staff. He or she also provides the resources to support the IT service management lifecycle and integrates the application management lifecycle into the IT service management lifecycle. The applications manager guides IT operations on ongoing operational management of applications (Office of Government Commerce, 2007:128-129).

Taking a broad view on the role of the applications manager (Baschab, Piot, 2007:322), he or she is also responsible form onitoring the performance and operation of applications, whether batch or on-line, real-time; application data integrity; application performance tuning; application patch management; and monitoring application integrity, that is, ensuring that the change and, release and deployment procedures are complied with as far as applications are concerned.

#### *4.5.5.1 Justification for Role*

The investment large organisations make in Enterprise Resource Planning (ERP) systems and other operational systems alone is sufficient justification to appoint a full-time manager to look after these multi-million-rand investments.

#### *4.5.5.2 Potential Role Combinations*

The skill set required to be an effective applications manager is very specific and different from that of most other functions, excluding perhaps aspects of the chief enterprise architect role, and more specifically, application architect.

### 4.5.6 Technical Manager

The technical manager is the custodian of technical knowledge and expertise related to managing the IT infrastructure. This role resources the technical infrastructure supporting the IT service management lifecycle, from service design through service operation and continual technology improvement. The technical manager is also responsible for guiding the operations manager on ongoing operational management of technology (Office of Government Commerce, 2007:121). It cannot be dictated whether the technical manager or the application manager owns and is responsible for the IT service support (Office of Government Commerce, 2000) and IT service delivery (Office of Government Commerce, 2001) processes, but it is required of these two roles to take responsibility for both of these between themselves.

#### *4.5.6.1 Justification for Role*

Technical infrastructure management is a specialised field that is very different from applications management and most other roles in IT.

#### *4.5.6.2 Potential Role Combinations*

Some organisations combine this role with that of the CTO or have a technical manager in lieu of a CTO. The nature of the operations manager role also makes that a possible combination with that of technical manager.

### 4.5.7 Operations Manager

The operations manager is responsible for:

- Operations control, including console management, job scheduling, backup and restoration, print and output management, recording and monitoring operational logs, and maintenance activities on behalf of application and technical management;
- Maintaining shift and operations schedules, managing and resourcing operational shifts, and maintaining reports on operational activities;
- Managing the physical environment (facilities), including data centres and recovery facilities, and, where required, managing consolidation of facilities;
- Maintaining and managing standard operating procedures, and ensuring compliance with operational service and infrastructural standards to maintain a stable operating environment; and
- Responding to business needs for scaling infrastructural capacity to levels that effectively support continually changing or expanding IT services (Office of Government Commerce, 2007:126-128).

#### *4.5.7.1 Justification for Role*

In a large IT environment, the number of operations staff and sometimes the number of facilities warrant the appointment of an operations manager.  This usually depends on the size of the organisation

#### *4.5.7.2 Potential Role Combinations*

Technical manager roles sometimes incorporate the operations manager role, though it might be difficult to combine it the other way round.  Technical management is more specialised and requires more than operations management experience.

### 4.5.8 RACI Mapping for Office of the CIO to IT governance major processes

Table 4.1 below maps the roles in the Office of the CIO to the five IT governance major processes, as interpreted by the researcher.  For each role, it is indicated whether that role is responsible (R) for, accountable (A) for, consulted (C) about or informed (I) of decisions and actions related to the major processes.  The term "RACI" relates back to this role clarification, that is, each role is R, A, C or I. Only one role can be accountable – the "buck stops" with that role.  The roles that are tasked with execution of a process are responsible.  In executing processes, other roles might be consulted or informed.

|  | CIO | CTO | ISO | Applications Manager | Enterprise Architect | Technical Manager | Operations Manager | IT Financial Manager | IT Risk Officer |
|---|---|---|---|---|---|---|---|---|---|
| Strategic alignment | A | R | I | C | R | C | I | C | R |
| Value delivery | A | C | C | R | C | R | R | R | C |
| Risk management | A | R | R | R | R | R | R | R | R |
| Resource management | A | R | C | R | I | R | R | R | C |
| Performance measurement | A | R | R | R | C | R | R | R | R |

**Table 4.1 – RACI Mapping for IT Management Roles**

Table 4.1 shows that all IT governance major processes can be managed by the proposed combination of roles mapped against the processes. The table indicates the CIO as being accountable for all IT-related matters, being the most senior IT manager in the organisation. In an ideal, balanced IT environment, the IT management team shares the responsibility for most aspects of IT management, with the balance swaying towards responsibility for most of what happens in IT, rather than contributing or being informed. An effective IT management team shares responsibility across the various disciplines.

## 4.6 IT Strategy Committee

The IT Strategy Committee is a board-level committee composed of Board members and non-Board executives, including the CIO. It assists the Board in governing and overseeing the enterprise's IT-related matters. It should ensure that IT governance is addressed formally and that the Board has the information it requires to ensure effective governance over IT (Office of Government Commerce, 2003:16). The Committee concerns itself with the alignment of IT to organisational objectives, more specifically, how IT delivers against strategy and how IT investments support the current and future needs of the organisation, as well as focusing IT on specific organisational objectives that are dependent on IT enablement (Office of Government Commerce, 2003:24). As such, the IT Strategy Committee is the highest IT governance body in the organisation.

### *4.6.1 Justification for Role*

Ali (2006:85) found that the existence of an IT Strategy Committee is positively correlated to the overall effectiveness of IT governance. Whether an organisation opts for a formal IT Strategy Committee or has a similar body for overseeing IT strategic planning and alignment, the need for the actions associated with a traditional IT Strategy Committee remains valid.

### 4.6.2 *Potential Role Combinations*

Some organisations take a different view of the IT Strategy Committee vs. the IT Steering Committee and interchange or combine roles as described in paragraph 2.3.3.3 below. Ross and Weill (2009:104) do not distinguish between an IT Steering and Strategy Committee but refer to a "senior management IT steering committee" comprising the firm's top executives.

## 4.7 IT Steering Committee

Board members often lack the knowledge to ask relevant questions about IT risk, expenditure and its contribution to competitive advantage. Recognising this, some US companies have established IT governance committees to oversee the governance of enterprise IT (Nolan, McFarlan, 2005:1-2). Surveys by the National Association of Corporate Directors (NACD) in the USA indicated Board members do not rate IT a major priority, and expertise in IT is not a highly valued attribute of new Board members. Executive management is expected to provide such oversight and only bring IT-related issues of significance to the Board on an exception basis (Marks, 2010:34).

The IT Steering Committee is at the executive level and focuses on tracking IT investment, setting priorities for IT and allocating scarce IT resources (IT Governance Institute, 2003:52). It typically combines senior business executives and IT management, with its membership often being indicative of the view of IT value in the organisation. Participation by executives is important to the success of an IT Steering Committee, as management's involvement has been shown to improve the effectiveness of IT governance in organisations (Ali, Green, Robb 2013). The Committee meets regularly to provide direction and oversight for IT across the enterprise. The IT Steering Committee is closely associated with IT service and project governance, and provides guidance and oversight for all other IT Steering Committees. Furthermore, it governs strategic functions including architecture, planning and vendor management (Cecere[a], 2009:1-2).

Luftman (2004:303) takes a different perspective, reducing the role of the IT Strategy Committee to setting the long-term IT strategy and stating that the IT Steering Committee business has the role of IT in the organisation, aligns IT with business, establishes IT investment principles, and sometimes establishes architectural principles and guidelines. This allocates most of the IT Governance Institute's view of the IT Strategy Committee to the IT Steering Committee. Nolan and McFarlan (2005:8) recommend that the IT governance committee be made up of non-executive directors, which has not been adopted widely in South Africa, due in part to the responsibilities borne by Board committee members, the availability of these directors to participate in the committee, and the accurate earlier observation by the authors that Board members often lack the experience to be effective IT governance committees, something the article later seemed to ignore. Overseeing IT governance through a Board committee makes sense in some instances, but should not be accepted as a generally recommended practice.

### *4.7.1 Justification for Role*

IT strategy needs to be driven to implementation, otherwise it remains theoretical. The IT Steering Committee oversees the selection of mechanisms to realise the IT strategy developed under guidance of the IT Strategy Committee.

### *4.7.2 Potential Role Combinations*

Elaborating on Luftman's view, it could be argued that the composition of the IT Steering Committee determines whether it could be combined with the IT Strategy Committee or not or whether the role of the latter could be reduced to mere setting of IT strategy. A senior IT Steering Committee would not be involved in the actual implementation of IT strategy, while a more operational IT Steering Committee would necessitate the need for segregation from the body that set the IT strategy so conflicts of interest are avoided. Combining the IT Steering and IT Strategy committees might be impractical in large organisations, where executives could find themselves unable to devote sufficient time to meet the increased responsibilities of a combination of the committees.

## 4.8 Enterprise Architecture Forum

As part of the Extended IT Organisation the Enterprise Architecture Forum focuses on the structure of the Extended IT Organisation and how it relates to the organisation overall (Office of Government Commerce, 2003:52). Top management, together with IT leadership, have the responsibility of establishing general enterprise architecture principles, while middle management and IT are responsible for enterprise architecture policy directives, and the architecture function itself for developing appropriate architecture models (Luipers, Van Steenbergen, Van Den Berg, Wagter, 2005:180). The Enterprise Architecture Forum is the body for achieving just that.

### *4.8.1 Justification for Role*

The topic of enterprise architecture has already received a great deal of coverage in this literature review, with sections 2.2.1.11, 2.2.4, 2.3.1.3.3 devoted to the topic, aside from this section promoting the creation of a governance body for the enterprise architecture function. Considering that enterprise architecture outlines the implementation of IT strategy, an Enterprise Architecture Forum is important to the realisation of the IT strategy. Architecture provides the blueprint for transforming organisations and the modernisation of technology (Suter, 2007:20).

### *4.8.2 Potential Role Combinations*

As this is a governance body it cannot be combined with any operational roles, however, the enterprise architecture function combines business and IT architectures.

## 4.9 Programme Management Office (PMO)

The IT PMO oversees the execution of programmes and projects in fulfilment of the strategic objectives of IT, as a sub set of the wider portfolio of projects in the organisation. The PMO also develops and enforces programme and project standards, reports on progress and assists in obtaining approval of project budgets (Rau, 2004:39). The IT PMO reports to the Enterprise PMO (EPMO), whose influence extends beyond one business unit or functional area (Kendall, 2003:40). In some organisations, the EPMO drives IT programmes and projects, while other organisations create an IT PMO for that purpose. Providing both apply strong programme and project management principles and follow consistent methodologies, there is little difference between the two approaches.

At the enterprise level, the portfolio management process aligns programmes (collections of projects with shared objectives) to organisational objectives. Diagrammatically, this could be depicted by three concentric circles, with the innermost circle representing projects, the middle circle programmes and the outer circle portfolios of programmes (Rajegopal, 2007:13). Any project management methodology should contain a project management maturity model, indicating maturity targets for project management. Crawford (2007:23-25) and Kerzner (2005:42) offer examples of such maturity models.

### 4.9.1 Justification for Role

A strategy is only as valuable as its translation into actions that contribute to the achievement of organisational objectives. Without an enabler to achieve this translation, strategy remains a theoretical subject. An IT PMO acts as such an enabler, translating the strategy into various IT programmes and projects.

### 4.9.2 Potential Role Combinations

Role combinations depend on the organisational approach to portfolio, programme and project management. In an organisation with an EPMO, the IT PMO could be part of the EPMO. For organisations that do not run sizeable IT projects, ad hoc PMO structures under the leadership of a senior IT manager could sometimes be sufficient. Some organisations even combine their EPMO and strategy functions, so the IT PMO could end up in Strategy.

## 4.10 RACI Mapping: IT Governance Structures to IT Governance Major Processes

The importance of clear, effective IT governance structures to oversee the functioning of the Enablers cannot be over emphasised. A successful IT governance framework will not only define the mix of Enablers but also the IT governance structures, complete with their accountabilities and responsibilities. There is no single, best organogram for IT. Depending on the organisation, a number of options exist, however, an IT department with all the roles researched in this section, is closely aligned to desirable practice and is more likely to be effective.

ITIL was the only desirable practice found to define clear roles for IT across the operational spectrum. COBIT was the only desirable practice found to specify clear roles across the strategic IT level, although the role descriptions were not very detailed. The segregation of and balance among operational IT management roles, oversight roles like those of the ISO and IT risk officer, and entity-level roles like the IT Steering Committee, IT Strategy Committee, PMO and Enterprise Architecture Forum remain challenges but will contribute greatly to IT governance if implemented successfully.

The RACI mapping of IT governance structures discussed above to the IT governance major processes is summarised in Table 4.2 below, with a mapping by the author:

| | Office of the CIO | IT Steerig Committee | IT Strategy Committee | Enterprise Architecture Forum | Pogramme Management Office |
|---|---|---|---|---|---|
| Strategic alignment | R | C | A | R | R |
| Value delivery | R | A | C | C | R |
| Risk management | A | I | I | C | R |
| Resource management | A | C | I | C | R |
| Performance measurement | A | I | I | C | R |

**Table 4.2 – RACI Mapping for IT Governance Structures**

Table 4.2 illustrates how the five proposed structures cover the entire spectrum of IT governance required by the IT governance major processes. As the ultimate IT governance body, the IT Steering Committee is accountable for the value delivery processes, that is, to ensure that IT serves as the enabler to business or the strategic differentiator to set the organisation apart from its competition. Strategic alignment of IT to the business is the accountability of the IT Strategy Committee, which in some organisations is combined with the IT Steering Committee.

As an operational body, the Office of the CIO is assigned accountability of all the operational processes and responsibility for the implementation of practical aspects of the other IT-related processes. The key enabler of IT initiatives, the PMO, takes some or all of the responsibility for implementing initiatives related to all IT processes.

## 4.11 Conclusion

This chapter discussed the organisational structures required for effective IT governance, with the responsibilities and accountabilities for each, as well as the parties who should be consulted or informed about aspects of the IT governance major processes. A summary of this is provided in Table 4.2.

# Chapter Five: Proposed New Framework

## 5.1 Abstract

The literature review presented in the preceding chapters provides the building blocks for a proposed IT governance framework. This chapter presents a proposed new IT governance framework.

## 5.2 Introduction

The definition of an IT governance framework adopted for this research is, "the underlying structure supporting IT governance through the combination of governance structures, architecture, processes, desirable practices and an IT control framework to effectively support the IT governance major processes". According to this definition, the components making up the "underlying structure" or framework are processes, governance structures, architecture, desirable practices and an IT control framework.

The five IT governance major processes were taken from the IT Governance Institute's model (2003:19) and are broken down into sub processes modelling all aspects of the IT environment. All governance structures, desirable practices and IT controls map back to the major processes, which in turn map back to the enterprise architecture. Governance structures are the roles, positions, governing bodies and structures overseeing IT governance in the organisation. The IT component (IT architecture) of the enterprise architecture reflects the composition of the organisation and the alignment of all architectural elements to organisational objectives. According to the definition adopted in this research, desirable practice is "the most appropriate practice accepted by consensus as a de facto standard or through certification as a de jure standard".

An IT control framework defines the underlying structure of the IT internal control environment, including all the most significant controls for the IT environment, together with the complementary, supporting controls.

## 5.3 Proposed Framework

Currently, there are arguments towards the fact that no universal framework exists that provides a single, cohesive view of all aspects of IT governance that is appropriate for most large organisations. The PES IT Governance Framework depicted in Diagram 5.1 provides such a single, cohesive view that could be populated to serve as a generic framework suitable for any large IT function. The proposed framework is structured around the three dimensions of a cube.

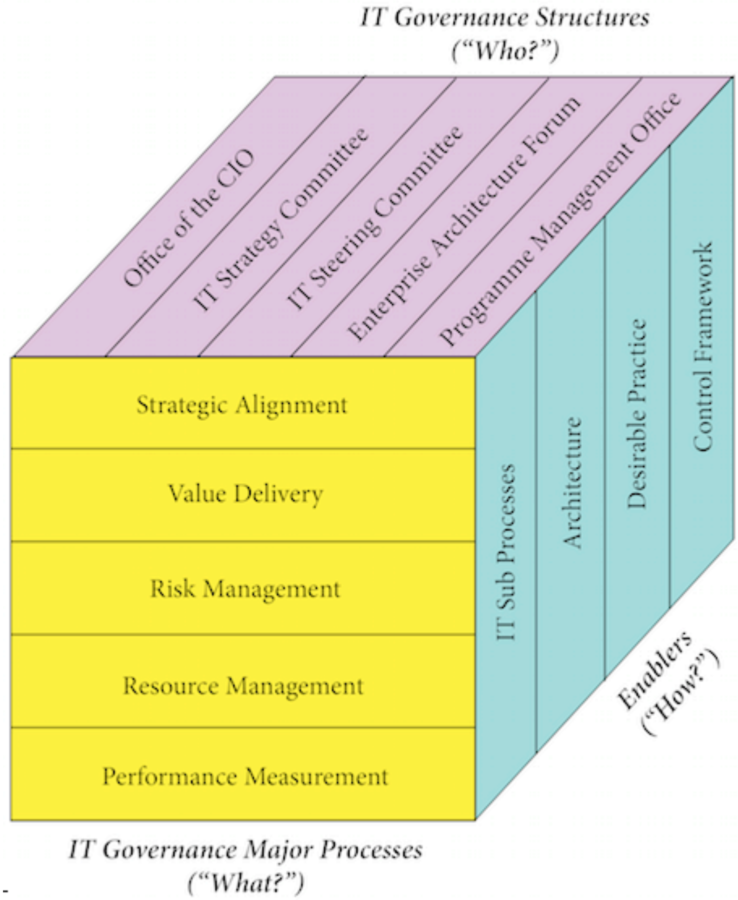


**Diagram 5.1 – Proposed PES IT Governance Framework**

The three dimensions of the PES framework are IT governance major processes, enablers and IT governance structures. The IT governance major processes have been taken from the IT Governance Institute's model (2003:19) and represent the high-level processes that form the foundation of the framework. These are to be used as the focal integration point of the IT governance framework. The major processes specify what should be done to practise sound IT governance, more specifically IT risk management, performance management, strategic alignment, resource management and performance management. Enablers for IT governance include the sub processes, architecture and control framework, all based on desirable practice, enabling the IT governance major processes. If the major processes are considered the backbone, the enablers are the muscles producing motion. The enablers are the embodiment of day-to-day IT governance and specify *how* sound IT governance should be practised. The IT governance structures specify who all are responsible and accountable for the effectiveness of the sub processes making up the five IT governance major processes.

## 5.4 Implementation Recommendations

Each of the three facets of the PES IT Governance Framework is now explained in greater detail, through the set of recommendations for implementation, provided below. These recommendations form the basis of interaction with the research participants, to evaluate whether they are practicable within the participating organisations. Being recommendations, the spirit of the PES IT Governance Framework is not one that insists on all recommendations being mandatory, but rather that they are customised for each organisation.

### 5.4.1 IT Governance Major Process Recommendations

#### *5.4.1.1 Strategic Alignment – Recommendation 1*

Strategic alignment between IT and business objectives forms the basis of sound IT governance. This alignment remains important throughout the IT organisation and the rest of the enterprise and could be achieved by implementing the following recommendations:

i. Organisations should have a formal IT strategy that is aligned to organisational objectives and that is updated at least annually;

ii. IT services should be aligned to the IT strategy, either informally or through formal enterprise architecture and service portfolio management mechanisms;

iii. Enterprise architecture and IT portfolio management should be considered as mechanisms for aligning IT and organisational strategies;

iv. An IT Strategy Committee or a combined IT Steering and Strategy Committee should be instituted to oversee the alignment of the IT strategy to the organisational strategy; and

v. The establishment of an Enterprise Architecture Forum should be considered.

#### *5.4.1.2 Value Delivery – Recommendation 2*

Recognising that formal value delivery practices are still in their early stages of maturity, it is recommended that a formal service level management process be adopted for defining value measurement criteria around key services, and that consideration be given to how ValIT could be used in support of value delivery in future. It is also recommended that the service level management process be formalised to closely monitor value delivery at the operational level; a PMO should be established to monitor significant IT projects; and the role of enterprise architecture should be considered as an enabler of value delivery.

#### *5.4.1.3 Resource Management – Recommendation 3*

It is recommended that the official organisational processes for resource management should be practised in IT and that specific processes be implemented for IT service management, project management (monitored via a PMO) and information security management.

#### *5.4.1.4 Risk Management – Recommendation 4*

It is recommended that a comprehensive IT risk identification and assessment process be implemented, as well as a formal IT control framework indicating the approved responses to all significant IT risks. The Risk IT framework started off as a draft publication to complement COBIT 4.1 and ValIT, but has since been integrated into COBIT 5. IT risk management should also be integrated with the enterprise risk management process.

#### *5.4.1.5 Performance Measurement – Recommendation 5*

It is recommended that an IT formal performance measurement process be implemented, whether in balanced scorecard fashion or using any other proven method.

### 5.4.2 Enabler Recommendations

#### *5.4.2.1 ITIL – Recommendation 6*

It is recommended that ITIL or a branded version of it, such as the Microsoft Operations Framework, be used when formulating IT service strategy, design, operation and general IT service management processes; when implementing a security management system as described by ISO/IEC27000; or when designing IT/business alignment mechanisms. ITIL supports the value delivery, resource management, risk management and strategic alignment major processes. ISO/IEC20000 is only recommended for organisations striving to achieve international ITIL certification, and does not directly support the proposed IT governance framework. The COBIT delivery and support processes, as well as the change and release management processes from the Acquisition and Implementation domain, directly support ITIL.

#### *5.4.2.2 COBIT – Recommendation 7*

COBIT 4.1, through the CMMI process maturity model, provides a comprehensive set of IT control objectives supporting the organisation's IT control framework, a high-level IT process map and an IT process maturity benchmark through its CMMI process maturity model. COBIT supports all five of the major IT governance processes. In terms of a proposed IT governance framework, it is recommended that the 34 processes in COBIT 4.1 be prioritised and that the following should be done for each key (high priority) process:

i. A procedure should be adopted to serve as the minimum level of formalisation of the process and as the basis for a consistent approach to the process;
ii. Where possible, desirable practice should be followed;
iii. Process maturity should be graded, using the CMMI grading included per COBIT 4.1 process;
iv. Key controls should be defined and implemented for the process, and staff should be trained on the effective use of each control; and
v. Input from internal and external audits should be sought on the design effectiveness of key controls.

#### *5.4.2.3 The ISO/IEC27000 Family of Standards – Recommendation 8*

ISO/IEC27000 (including ISO/IEC17799) represents desirable practice for information security management systems and control guidance. It is recommended that organisations which have achieved a level four COBIT 4.1 process DS5 CMMI maturity should consider formally implementing ISO/IEC27000, however, all organisations would benefit from consulting the control objectives and controls proposed by ISO/IEC27000, when implementing process DS5. ISO/IEC27000 should be considered in support of the risk management major IT governance process.

#### *5.4.2.4 Balanced Scorecard – Recommendation 9*

Organisations are encouraged to consider the balanced scorecard as a performance measurement mechanism, but should adopt some performance measurement tool to address the IT governance major process, performance measurement, in the PES IT Governance Framework.

#### *5.4.2.5 Prince2 and PMBOK – Recommendation 10*

As the definitive work on project management, it is recommended that PMBOK be used as the project management standard for organisations adopting the generic IT governance framework, with a project management method such as Prince2 for comprehensive project management processes. PMBOK supports the Strategic Alignment major process; more specifically, COBIT process PO10. Organisations have a number of project management methods, so any structured method could be used if Prince2 is not adopted.

#### *5.4.2.6 TOGAF – Recommendation 11*

It is recommended that organisations explore ways of formalising their enterprise architecture through the use of frameworks like TOGAF and the work of Weill and Ross. Enterprise architecture is a growing, maturing field and, at this stage, there is no clear, single answer. Enterprise architecture supports the Strategic Alignment major process.

#### *5.4.2.7 VALIT – Recommendation 12*

It is recommended that the Value Delivery major IT governance process be implemented using ValIT, to formalise value management practices and align IT portfolio management to corporate portfolio management processes.

#### *5.4.2.8 King III Report – Recommendation 13*

Where the organisation has decided to implement the recommendations of the King III report, it is recommended that the following be implemented to fulfil the requirements of the IT governance chapter of King III:

i. A Board IT governance awareness programme should be undertaken to ensure the directors understand all aspects of IT governance, for which they are accountable.

ii. An IT charter should be established, setting out the objectives of the IT function in support of organisational objectives, including sustainability objectives, and governance requirements of the IT function. The charter should also define all key IT governance structures and roles, as well as their decision making responsibilities and accountabilities.

iii. A set of policies, procedures and standards should be implemented to guide behaviour in IT, in line with the IT charter.

iv. A formal IT risk management function should be implemented, with the CIO being accountable for effective IT risk management and a specific person being responsible for ensuring compliance with the required IT risk management practices. Under this process a formal IT risk register should be implemented.

v. An IT internal control framework should be implemented, to match the IT risk register. The controls should be designed to clearly specify what actions are to be undertaken, at what frequency, by whom, and what evidence of executing these actions should be retained.

vi. IT should be awarded a dedicated section of the integrated report required by King III, with regular IT submissions being made.

vii. A formal IT strategic planning process should be implemented, including a procedure for the continual realignment of the IT objectives to those of the organisation.

viii. The impact of IT on society and the environment should be considered and how IT could promote sustainability.

ix. An IT governance framework should be established for the organisation, providing guidance on the process, structures and practices to be implemented to achieve effective IT governance.

x. An IT Steering Committee should be established to oversee IT investment, priorities and resource allocation, on behalf of the Board.

xi. The CIO should be the single point of accountability for IT to the Steering Committee.

xii. An IT Strategy Committee should be established or the combined responsibility for IT strategy and IT investment, priorities and resource allocation should be made the combined responsibility of the IT Steering Committee, to involve the Board in strategic IT decisions.

xiii. The IT Steering Committee should monitor significant investments for value in terms of IT strategy and appropriateness of resource allocation to the investment. Compliance with the procurement policy should also be monitored.

xiv. An IT vendor management process should be implemented.

xv. At a minimum, a basic IT value management process should be implemented. Where feasible, IT portfolio management should be implemented to track the value derived from IT investments.

xvi. IT should submit regular reports to the IT Steering Committee to enable the Board to monitor the execution of the IT strategy and IT service delivery in general.

xvii. A risk assessment process should be implemented that requires at least an annual, comprehensive IT risk assessment and regular updates to the IT risk understanding, all of which are documented and monitored in a formal IT risk register.

xviii. The agendas of all risk and audit committee meetings should provide for a section on IT-related risk and control reporting.

xix. Business continuity management should not be regarded as an IT responsibility, but IT should be able to clearly demonstrate how its IT service continuity planning satisfies business continuity management requirements, as is expected of all departments in the organisation.

xx. Formal information management practices should be implemented to monitor the quality of data and information, compliance with privacy regulations and stakeholder requirements, and information security management.

xxi. An IT compliance framework should be implemented to ensure that all IT stakeholders', legislative, regulatory and corporate requirements are met.

#### *5.4.2.9 ISO/IEC38500 – Recommendation 14*

i. An IT role player matrix should be implemented, showing the responsibilities and accountabilities of all roles, as well as which roles need to be consulted or informed in the performance of IT duties.

ii. Performance management should be implemented at staff, structure and process levels, to monitor how responsibilities are being fulfilled.

iii. An IT PMO should be implemented if no EPMO exists to manage all projects, including those in IT. The PMO accepts responsibility for the implementation of IT projects.

iv. The systems development lifecycle and project management methodology should be formalised, as mechanisms for implementing strategy.

v. A process should be implemented for integrating IT strategic planning and the operation of the IT PMO, to translate IT strategy into execution.

vi. An enterprise architecture function should be implemented to blueprint core aspects of the business and the manner in which IT should enable it.

vii. IT infrastructure management should be implemented, with renewal plans to ensure that the execution of IT strategy is sustained at an infrastructural level.

viii. Strategic sourcing should be practised as part of the IT vendor management process.

ix. An IT assets lifecycle management process should be implemented to support IT planning and ensure the optimal use of IT assets.

x. Formal IT service support and service delivery processes should be implemented to ensure consistent, efficient IT services.

xi. The key IT metrics should be defined, monitored and reported on an ongoing basis.

xii. Formal processes should be implemented for IT planning, IT service management, project management, the systems development lifecycle, information security management, IT risk management, and enterprise architecture.

xiii. Risk and control self assessment should be implemented as a mechanism to continually monitor compliance.

xiv. IT roles and responsibilities should be formalised, including the following:

a. Formal job descriptions should be implemented.

b. Incompatible duties should be segregated.

c. Performance management should be practiced in line with job descriptions.

d. Formal planning should be done for skills development and retention.

e. Formal performance management should be implemented.

#### *5.4.2.10 IT Sub Processes – Recommendation 15*

It is recommended that sub processes for the IT environment be formalised under each of the IT governance major processes in line with the desirable practices recommended in this paper. Each process should be supported by policies, procedures and standards setting out the mechanisms, structures and controls for effective operation thereof.

#### *5.4.2.11 IT Control Framework – Recommendation 16*

As part of the proposed IT governance framework, it is recommended that IT controls should be formalised in an IT control framework, based on the COBIT 4.1 control objectives and other relevant control objectives, for example those contained in ISO/IEC27000, for information security. The COBIT sub paragraph above dealt with COBIT in detail.

#### *5.4.2.12 Supporting Documents – Recommendation 17*

It is recommended that the policies, procedures and standards required to govern each key (high priority) process be formalised, that a risk assessment be performed to highlight all high risk areas and that an IT control framework be implemented to mitigate the identified risks. These documents should be reviewed and updated at least annually. The ultimate accountability for the effectiveness of policies, procedures and standards, and for the execution of risk assessments, resides with the CIO.

#### *5.4.2.13 Architecture – Recommendation 18*

Enterprise architecture (EA) is an important mechanism for integrating IT and the business. The proposed IT governance framework recommends that organisations should at a minimum embark upon an exercise to investigate an appropriate approach to EA and to document their findings for consideration once the organisation has reached a level of maturity where a formal architecture function becomes feasible. The framework is not prescriptive about the roles within the EA function or what reporting lines should be followed, but recommends the formalisation of the EA organisation, together with its roles and responsibilities.

#### *5.4.2.14 Portfolio Management – Recommendation 19*

Recognising the developing nature of portfolio management, it is recommended that organisations:

i. Explore how portfolio management will be utilised in future IT investments and management;
ii. Establish a mechanism to align IT spend (and related projects) to organisational objectives;
iii. Take note of the development and maturing of the ValIT framework; and
iv. Consider how the ITIL Service Portfolio management process could benefit the organisation.

#### *5.4.2.15 Desirable Practices – Recommendation 20*

As depicted earlier in Table 3.2, it is recommended that the IT governance major processes are implemented using the following desirable practices:

i. Strategic alignment: COBIT, ITIL, TOGAF, portfolio management, King III and ISO/IEC38500.
ii. Value delivery: COBIT, ITIL, PMBOK, Prince2, portfolio management, King III and ISO/IEC38500.

iii. Risk management: COBIT, ITIL, ISO/IEC17799/ ISO/IEC27001, portfolio management, King III and ISO/IEC38500.

iv. Resource management: COBIT, ITIL, PMBOK, Prince2, King III and ISO/IEC38500.

v. Performance measurement: COBIT, balance scorecard, King III and ISO/IEC38500.

### 5.4.3 IT Governance Structure Recommendations

#### *5.4.3.1 Office of the CIO – Recommendation 21*

The PES IT Governance Framework does not insist on the existence of a CTO role. Rather, it is recommended that either the definition of the CIO role should be broadly defined to incorporate the role of the CTO or the roles of the CTO and CIO should be clearly segregated. The CIO role is rapidly changing and needs to be adjusted continually to keep up with new demands. Each organisation should define the CIO role to meet its strategic requirements of IT. These requirements would determine the value IT should deliver and consequently the role of the individual leading the function.

#### *5.4.3.2 Chief Technology Officer (CTO) – Recommendation 22*

It is recommended that the creation of a CTO role should be based on a strategic decision and the nature of the organisation. Not all organisations are able to justify a CTO role. Organisations which have made a significantly higher investment in IT infrastructure than their peers, as well as telecommunications organisations, would probably find it easier to justify a CTO role.

#### *5.4.3.3 Information Security Officer (ISO) – Recommendation 23*

The ISO role should be clearly defined and segregated from the implementation and administration of these policies, procedures and standards, as the most senior information security oversight function. If possible, it should be based outside IT.

#### *5.4.3.4 Chief Enterprise Architect – Recommendation 24*

It is recommended that organisations' IT strategies make provision for the creation or maturing of the EA role. Where feasible, this role should not be regarded as an IT function but should rather be based closer to corporate strategy, with its technology-specific roles being resourced from IT.

#### *5.4.3.5 IT Financial Manager – Recommendation 25*

It is recommended that the IT financial management role be formally assigned in all environments but that the feasibility of creating a full-time position around it be carefully evaluated based on the size and complexity of the environment.

#### *5.4.3.6 IT Risk Officer – Recommendation 26*

It is recommended that a formal IT risk officer role be created. Depending on the organisation, it could then be decided whether to award this role as an additional responsibility to a senior IT official or to create a new position within IT for an operational risk manager. It is further imperative that all of the IT management team be made aware of their risk management responsibility.

#### *5.4.3.7 Applications Manager – Recommendation 27*

It is recommended that, where feasible, the role of application manager should not be combined with other formal roles in large IT departments.

#### *5.4.3.8 Technical Manager – Recommendation 28*

The proposed IT governance framework recommends that the technical management role be clearly defined and assigned to an individual responsible for all aspects of technical management. The framework does not dictate whether the technical manager or the application manager owns and is responsible for the IT service support (Office of Government Commerce, 2000) and IT service delivery (Office of Government Commerce, 2001) processes, but requires these two roles to take responsibility for service support and service delivery between the two of them.

#### *5.4.3.9 Operations Manager – Recommendation 29*

It is recommended that each organisation evaluate whether or not the size of its IT department justifies the appointment of an operations manager. If not, this role could be combined with that of the technical manager. This paper does not argue for any particular IT operations structure but recommends (i) clear roles and responsibilities for each operational area and (ii) a clear definition of the operations management role.

#### *5.4.3.10 IT Strategy Committee – Recommendation 30*

It is recommended that all organisations should have an IT Strategy Committee, composed of top executives and the CIO. In some organisations, this committee would also be responsible for areas assigned to the IT Steering Committee below.

#### *5.4.3.11 IT Steering Committee – Recommendation 31*

It is recommended that each organisation should have at least one IT governance body responsible for setting IT strategy (IT Strategy Committee) and one for overseeing the establishment of mechanisms for delivering the strategy (IT Steering Committee). Where feasible, these should be two different bodies but, provided the body does not involve itself in the actual implementation of strategy, the two could be one. Where the two bodies are segregated, the IT Strategy Committee membership should be as senior as possible, preferably Board level.

#### *5.4.3.12 Enterprise Architecture Forum – Recommendation 32*

It is recommended that some kind of governance body be established to oversee the establishment and effectiveness of enterprise architecture in the organisation. Where possible, this function should be situated outside IT, as a corporate strategy implementation enabler.

#### *5.4.3.13 Programme Management Office (PMO) – Recommendation 33*

Without being prescriptive as to where the IT PMO should reside, it is recommended that PMO principles be adopted to govern any significant IT projects. It is further recommended that a formal, standardised project management methodology, including a project management maturity model, whether for IT or at an enterprise level, be adopted. The adopted project management methodology should contain a project management maturity model, indicating maturity targets for project management.

#### *5.4.3.14 Summarised Recommendation on IT Governance Roles – Recommendation 34*

As depicted in Table 4.1, it is recommended that the IT governance major processes are implemented by assigning responsibility to the following IT governance roles: CTO, ISO, applications manager, enterprise architect, technical manager, operations manager, IT financial manager and IT risk officer. The CIO is assigned accountability for all these roles performing their responsibilities.

#### *5.4.3.15 Summarised Recommendation on IT Governance Structures - Recommendation 35*

As depicted in Table 4.2, it is recommended that the IT governance major processes are implemented by assigning responsibility to the following IT governance structures: office of the CIO, IT Steering Committee, IT Strategy Committee, Enterprise Architecture Forum and PMO.

The IT Strategy Committee is acountable for ensuring strategic alignment, while accountability for value delivery is assigned to the IT Steering Committee. The office of the CIO is accountable for the remaining three IT governance major processes.

## 5.5 Conclusion

Being a proposed IT governance framework, the intention for users of the PES IT Governance Framework is to implement the recommendations relevant to their organisations to achieve effective IT governance. In subsequent chapters, this framework forms the basis for discussion with research participants and the eventual formulation of a generally accepted IT governance framework.

# Chapter Six: Design of the Empirical Work

## 6.1 Abstract

The previous chapter proposed the PES IT Governance Framework, supporting the empirical work, while chapter six sets out its design.

## 6.2 Introduction

The purpose of this research is to formulate a generic IT governance framework that can be used by any large corporate environment. This section describes the research design, methodology, limitations, and ethical considerations, followed by a conclusion.

## 6.3 Research Design

The research is structured around the PES IT Governance Framework, which has its origins in a 2004 article written by the researcher for the IA Adviser. The concept of a generic IT governance framework was discussed with a number of CIOs before the researcher consulted existing literature on IT governance, as the basis for compiling a theoretical IT governance model. Ten CIOs were then interviewed, each completing a questionnaire. Their contributions were analysed and served as input for the production of an amended PES IT Governance Framework.

The strength of this approach lies in its balance between the theoretical IT governance framework and the interviewees' years of experience. Any impracticality in the proposed framework is exposed through the interviews and can be addressed to arrive at the final framework. Obtaining input from a group of senior executives through a questionnaire could be too simplistic or restrictive to obtain meaningful responses (Webb, 2000:199), however, using the discussion paper as the common reference for questionnaires requires the CIOs to consider the proposed framework beforehand. The questionnaire then allows them to respond to a number of focused open-ended questions that create the ability to provide sufficient detail. The South African CIOs included in the process represent a homogenous group of stakeholders in the IT governance process, so meaningful inferences from their opinions can be drawn. The process was designed as such to avoid problems that could arise when analysis has to mediate widely different input from various organisational levels and geographies.

Open-ended questions are phrased carefully to address a specific topic to avoid lengthy exposition that only addresses the subject in general, without adding the required perspective (Webb, 2000:205). When recording responses to open-ended questions, the interviewer takes care to record responses verbatim and not let personal bias or interpretation interfere with the integrity of input. Open-ended questions are analysed individually, which increases the time and cost of analysis. An additional challenge when dealing with senior executives is their availability and the amount of time they are able to allocate to research interviews. Too many open-ended questions could result in them not being willing or able to devote a meaningful amount of time to the research efforts.

Closed-ended questions enforce a structured response, which could be ineffective when overly restrictive (Webb, 2000:205). Conversely, when used appropriately, they can be very effective at sourcing responses to clear-cut questions. For the purposes of this research, closed-ended questions are invaluable to confirm the working draft of the PES IT Governance Framework, as the various inputs can be analysed more easily in order to confirm the theoretical, literature review-based IT governance framework used as the basis for interviews.

## 6.4 Methodology

The research followed an iterative approach. After an introductory conversation with participants and consideration of a variety of literature, an initial version of the PES IT Governance Framework was produced. The contents of the framework was reduced to a questionnaire, through which the participating CIOs provided feedback. The questionnaire included a general section to confirm various aspects of the framework, while a section for each of the five IT governance major processes confirmed the practicable structures, roles and mechanisms to achieve strategic alignment between IT and business, delivery of value through the investment in IT, as well as effective IT risk management, IT resource management and IT performance measurement. The participating CIOs' comprehensive input was then analysed and the PES IT Governance Framework updated, which constitues the final product of the research.

This methodology challenges the theory summarised during the literature review in a real-life application. The emphasis is on generic IT governance, which requires practical input to satisfy these criteria. A variety of organisations are involved to explore the generic application and reach agreement on the content, to ensure sustainability. Input from participants is then aggregated and the majority view incorporated into the draft PES IT Governance Framework to produce the final framework.

## 6.5 Research Instruments

IT governance draws on the culture, ethics and integrity of an organisation's leadership. As such, its design and effectiveness depends greatly on leadership. To arrive at a practicable end product with useful application in the real world, it was decided to prepare a theoretical IT governance framework and subject it to criticism by ten CIOs, in the form of structured questions embedded in the IT governance framework discussion paper, to be responded to during interviews.

CIO responses are elicited through a combination of open-ended, less structured questions and a very structured, predominantly closed-ended questionnaire that seeks specific validation of the structures, processes, practices, roles and mechanisms proposed in the generic framework. The quality of input depends on the quality of participants in the process, in this case CIOs from large South African companies.

The questionnaire was designed to extract the participants' views on the detail required to implement each of the PES IT Governance Framework's dimensions, reducing the recommendations in the discussion draft to a set of questions to gather the necessary qualitative and quantitative input. The questionnaire was presented in spreadsheet format to allow for validation of the completeness of input, and to enable ease of comparison and interpretation of data.

## 6.6 Data

The population was defined as a group of ten CIOs, five from public sector South African (SA) entities and five from private sector SA companies, from organisations with a turnover or, in the case of public entities, a budget, in excess of R1 000 000 000 (R1 billion) per annum. The interviewees were not selected randomly but rather based on the interviewer's access to them and their significance in the SA corporate community and government. Considering the entire population of organisations with a turnover or government budget over R1bn per annum, the ten organisations provide a spread representing a significant portion of IT spend in South Africa, which is adequate for the purposes of this research, as the emphasis is more on sourcing practical input from top IT officials than performing statistical analysis. The researcher's direct involvement in every interview ensured data quality, as said researched engaged with the interviewees, capturing their inputs throughout the interview and verifying data captured through the use of control totals. The strength of the data lies in its source, being top IT officials from each of these organisations, with the participants capturing most of the data themselves and the researcher verifying the capture sheets with the interviewee afterwards, where necessary. The significant qualitative portion of data may be of limited use for statistical analysis, but the research objectives are not directed at such analyses, so the data set is deemed adequate.

## 6.7 Analysis

Effective IT governance is not an exact science that could be applied uniformly across different organisations. The formulation of the PES IT Governance Framework therefore relies on a combination of theory and practical application, based on the experience of senior executives who have successfully run IT organisations, implementing the governance structures and processes to align IT to business, generate value through IT investment and operation, and manage IT risk. To achieve this, each participant's comment is considered during the finalisation of the framework. The structured input sourced through the questionnaire accompanying the draft IT governance framework presented to the participants, is aggregated into a single spreadsheet to validate the preferred processes, structures, roles, mechanisms and practices, and update the framework accordingly.

The structured input is analysed in three categories, comprising questions rated on a five-level scale, a binary scale and a variable scale. The first catergory includes recommendations suggested by the PES IT Governance Framework that are rated on a five-level scale of importance, including *critical, very/highly, important/valuable, somewhat* and *none not at all*. Every question has ten inputs reflecting a single choice across the five levels. If five or more participants select *critical* or *very/highly* important, the recommendation is rated as *Accepted,* if five or more select *critical, very/highly* or *important/value,* the recommendation is *Considered* for inclusion in the framework, otherwise it is *Not Accepted* and excluded from the framework. The second category requires participants to make a binary selection between two options , where the recommendation is either *Accepted* or *Not Accepted.* Finally, there are recommendations that span a number of different options, where more than five candidates' preference of an option indicates them to be *Accepted,* five results in them being *Considered* and fewer than five, *Not Accepted.* Based on a combination of the participants' comment, responses to the questionnaire and the researcher's experience, the final IT governance framework is then formulated.

## 6.8 Alternative Approaches

Alternatives to the approach adopted for this research were considered, include targeting a group of companies with questionnaires directed via e-mail, and following a purely theoretical approach, based on IT governance publications and articles, formulating theories about the most appropriate application to organisations mentioned in the articles.

### 6.8.1 Targeting a Sample of Companies

Following this approach, an Internet-based email survey engine would have been used to send out questionnaires for completion and return to the researcher. The South African chapter of ISACA offers such a service, which targets their members and which may produce a reasonable response, albeit from less senior, assurance-focused officials at the companies employing them. Alternatively, a sample of JSE-listed companies could have been selected and an email survey sent to the company secretary, requesting a response from the CIO. Previous attempts to contact CIOs where there was no direct link or reference to the official yielded poor results. Considering the degree of difficulty committing the CIOs in the research group to this research, an approach relying on emails to a company secretary is not likely to result in a high response rate. Furthermore, basing research deductions on a purely theoretical survey without direct contact is likely to produce a less practicable framework. Relying on junior officials will also not produce an in-depth result.

### 6.8.2 Theoretical Approach

An approach that relies purely on IT governance publications and articles to formulate theories about the most appropriate application to organisations mentioned in the articles could lead to a result, albeit one that would not be very practicable. During the literature review, few articles were found that would support this approach. If these approaches were feasible they would have simplified the research, as they eliminate the need to find CIOs willing to participate in the process. On the other hand, the researcher who does not have a network of CIOs might find it very difficult, if not impossible, to involve a sufficient number of CIOs to make the research meaningful.

## 6.9 Limitations to Reliability and Extent

The extent to which the research results could be generalised is positively influenced by the fact that the research group targeted did not represent a particular industry only; were from a combination of government, parastatal and private sector companies; were not selected mainly from industries where specific frameworks could skew the IT governance perspective to an industry-specific extreme, for example, the eTOM framework for the telecommunications industry; and that the research was based on generally applied international frameworks. however, generalisation is limited to South African organisations with a turnover or, if not private sector, a budget in excess of R1bn per annum. It is further based on the opinions of CIOs and therefore could not be generalised outside the context of the IT function, despite its usefulness as a complementary study to corporate governance.

No significant limitations to reliability of the data collected were identified during the course of this research. Despite the limitations to usefulness as a generalised study mentioned above, the findings are still valuable because they were guided by internationally desirable practice and tested by subjecting them to senior IT professionals in large, prominent South African organisations.

## 6.10 Ethical Considerations

The research undertaken requires input from ten organisations on IT governance-specific aspects. To avoid conflicts of interest and ethical conflicts, the following considerations were built into the selection of the organisations interviewed:

i. None of these organisations competes directly with any other organisation interviewed;

ii. All interview results are individualised and fed back to each organisation interviewed, as an incentive for each organisation to cooperate fully for the value they are realising in the process;

iii. Individualised instances of results are not shared across interviewees;

iv. Reports on interviews reflect the group position only and individual organisations are never highlighted without the express permission of the organisation;

v. No information solicited is so specific that it could compromise the security, continuity or competitive advantage of any of the organisations, even if a third party with malicious intent should obtain the interviews.

To ensure confidentiality, organisations' input is not included under each organisation's name but rather referenced from one to ten. No configuration-specific information is obtained during the research that could compromise any of the participants. This applies to listing specifics about enterprise architecture, including all architecture layers.  The research only shares the total analysis across participants, without revealing the names of organisations that choose to remain anonymous to other participants.  The researcher signs non-disclosure and confidentiality agreements, as required, and undergoes any security procedures necessary.  The research discussion paper and questionnaires are made available at least three weeks prior to the interview to assure the CIOs that no compromising questions are asked.  No deviations from the University-approved discussion paper are entertained during the interviews.  Furthermore, any discussion around the participant's involvement in this research is between the student and his supervisor only.  Participants choosing to remain anonymous are not mentioned in the research or any subsequent related publications, except as an anonymous institution meeting the research criteria and approved by the supervisor.  As part of the sanction of the research proposal, tthe Faculty approved the approach of interviewing ten CIOs.  There is potential for sensitivity, especially among the government participants, but all reasonable attempts have been made to counteract concerns.

## 6.11 Conclusion

The empirical work has been designed in such a manner that it combines IT governance theory with the experience of a group of participating CIOs from large organisations, thus yielding a product that could be useful to them post the publication of this research.  The results and analysis contained in chapters seven and eight reflect on the outcome of the participant interviews, analysis of their input, conclusions about recommendations to be included in the IT governance framework, and the update to the framework itself.

# Chapter Seven: Results of the Empirical Work and Analysis of Results

## 7.1 Abstract

The previous chapter covered the empirical work design, while chapter seven presents the results and analysis of the empirical work.

## 7.2 Introduction

This section focuses on the outcome and interpretation of participant input. Most of this took place while aggregating input into a single sheet, which is presented as an appendix to chapter seven. All input has now been considered before the final IT governance framework is prepared, with cross-references between the structured input and the recommendations in the final framework presented in Appendix Three. Participant comment has been summarised, thus both structured and non-structured input can be considered in preparing the final framework, which is presented in the next chapter.

## 7.3 Respondents

Ten organisations were selected to provide representation across both the private and public sectors. In the public sector group, the CIOs of a financial services and metropolitan utility participated, while three other organisations delegated the interviews to specialist IT governance senior managers on their IT executive, including an academic, telecommunications and financial services organisation. The senior managers were involved, as they were regarded as being more specialised, with the impression created that they were deemed to be more knowledgeable on the specifics of the topic than the CIOs.

As for the public sector group, the metropolitan utility is Johannesburg-based, while the two financial services, telecommunications and academic organisations are situated in Pretoria. Thus, all public sector participants came from Gauteng. These are all more progressive government institutions in the sense that they are not traditional government departments but rather specialised agencies and organs of state that are more respected in the market than most departments. As such, they were expected to have an understanding of IT governance concepts.

In the private sector group, CIOs of mining, media, metals, life assurance and banking organisations participated. An interesting difference from the public sector participation is that all the private sector CIOs availed themselves to take part in the research interviews. This might be interpreted as a higher degree of confidence in their understaning of IT governance concepts than the public sector CIOs. One company is based in the Northwest (Marikana), one in the Western Cape (Cape Town) and three in Gauteng (two from Johannesburg and one from Vereeniging).

All ten of the interviews were constructive, with much comment about recommendations, which allows for meaningful refinement of the proposed framework. There were no negative responses, with participants indicating that they found the experience interesting and some even requesting to quote from the discussion paper.

## 7.4 Interview Analysis

All participants' comment was considered before the summary below was prepared, reflecting the evaluated suggestions that make sense for a generic IT governance framework. No comment was received that contradicted the framework or challenged it in a destructive manner, so provision was made to accommodate all input in the updated PES framework.

### 7.4.1 General and Overarching Comment

Participants had a free text section to provide general comment before responding to more structured recommendations. These suggestions have been summarised into seven points, presented below:

1. Emphasise the need for identifying relevant aspects of practices and standards rather than applying them wholesale or being overly prescriptive. Clarify whether there are mandatory and discretionary components to the framework. Do not be overly rigid. This became a theme throughout the comment provided by participants.

2. Highlight the importance of compliance, including regulatory requirments, King III and the Sarbanes-Oxley Act. This is becoming increasingly important, as the regulatory burden grows year on year. Regulatory pressure has grown throughout the period of this research and has become an important aspect of IT governance.

3. Better contextualise IT and corresponding business functions, such as IT service continuity management vs. business continuity management and IT architecture vs. the other architecture layers. Provide the perspective so it becomes clear what aspects of IT governance are embedded in business functions and what aspects need to be treated as IT-specific functions. The reality is that IT is still being presented with responsibilities that sound governance would require business to take up, yet they regard IT as better skilled to take care of these areas, such as enterprise architecture and information security governance.

4. Emphasise the importance of organisational change management, because effecting sound IT governance depends mostly on behavioural change. Effective change management is a critical success factor for bringing about effective IT governance. It is more of an implementation imperative than part of the framework, but has been mentioned in the update to the original framework.

5. Explain that organisational culture influences the adoption of IT governance structures, mechanisms and processes – something which COBIT 5 echoes. Combining change management with cultural awareness and sensitivity is highly important to successful implementation of the IT governance framework.

6. Provide clearer context to the users of the PES framework, more specifically around:

    a. How the IT governance framework was derived;
    b. Business intelligence and information management;
    c. Business relationship management and demand management;
    d. Whether there are mandatory and discretionary components to the framework. Do not be overly rigid.

    All of these were meaningful suggestions and have been included in the updated framework.

7. Update the PES cube to include the Board and ensure the cube remains aligned to the narrative after all updates following participant interviews have been made. This was a critical omission in the initial framework and has been rectified.

#### *7.4.1.1 Recommendation 1 – Strategic Alignment*

Recommendations received: 4

Much of the comment received requested more specific guidance on how to implement aspects of IT governance, rather than what should be done. This requires a fine balance to avoid producing an over-prescriptive framework that would not be generally suitable. The comments received could be summarised into two requirements: one, to provide for a formal strategic alignment process, rather than a vague requirement for strategic alignment, including the prioritisation of strategic initiatives; two, to emphasise the importance of architectural alignment, with IT being responsible for the IT layer. This is important, as the IT layer needs to be distinguished from the non-IT architectural responsibilities.

#### *7.4.1.2 Recommendation 2 – Value Delivery*

Recommendations received: 5

In the researcher's experience, value management has been the most difficult aspect of IT governance to implement. The initial draft suggested return on investment (ROI) as a means of calcuating value delivery, but the participants pointed out that the topic should not be reduced to a mere ROI calculation. Instead, the importance of benefits formulation (most importantly, contribution to strategy execution), monitoring and reporting should be emphasised. As a means of monitoring the generation of value, provision should also be made for alignment of the programme management office to business structures and segregation of the programme management officefrom delivery.

#### *7.4.1.3 Recommendation 3 – Resource Management*

Recommendations received: 7

Most participants provided comment on this recommendation, ranging from the need to emphasise recommended roles rather than the creation of positions and clarifying what is meant by "resources", to providing more prominence to people processes. Contextualisation of vendor management and outsourcing, as part of the resource management major process, were also deemed important. It is essential to note the importance of both people and cultural aspects, as COBIT 5 also highlighted.

#### *7.4.1.4 Recommendation 4 – Risk Management*

Recommendations received: 4

Participants regard IT risk management as a sub set of enterprise risk management (ERM) and requested emphasis on this integration. Another need expressed was for the contextualisation of IT governance against the other combined assurance stakeholders, including the internal audit, external audit, ERM and compliance functions.

#### *7.4.1.5 Recommendation 5 – Performance Measurement*

Recommendations received: 2

Most participants agreed with the recommendation as it stood, with two of the CIOs suggesting more detail. The importance of communicating strategy, combined with using IT scorecards as tactical and operational tools for measuring strategy execution and general performance against the IT governance major processes, was highlighted.

#### *7.4.1.6 Recommendation 6 – ITIL*

Recommendations received: 3

Three participants requested additional contextualisation of the use of standards and practices in support of IT governance. As standards and practices are the life blood of an organisation's IT governance framework, it is important that users of the framework have a clear understanding of the relevance of standards and practices to each aspect of IT governance, and how they should be combined to achieve effective, yet practicable IT governance.

There was a specific request to position COBIT 4.1 and ISO/IEC38500, both of which were key inputs to the formulation of COBIT 5. It is a reality that many organisations have not yet made the transition from COBIT 4.1 to COBIT 5 and as such, clarity should be created regarding how the two publications could be used inidividually or in combination. On its own, ISO/IEC38500 never gained the expected momentum, serving instead as an important building block for COBIT 5.

#### 7.4.1.7 Recommendation 7 – COBIT

Recommendations received: 1

The only input here was to update the ITGI report reference from 2008 to the more recent 2011 edition.

#### 7.4.1.8 Recommendation 8 – The ISO/IEC27000 Family of Standards

Recommendations received: 1

The request here was again for clarification as to how the standard should be supplied in the implememtation of the framework, without making it a rigid requirement.

#### 7.4.1.9 Recommendation 9 – Balanced Scorecard

Recommendations received: 5

The suggestions here emphasised the need for performance management, monitoring and reporting, rather than be prescriptive that it has to be a balanced scorecard. The participants require a framework with clear guidance, but not something too rigid that would not be easy to implement in a generic context.

#### 7.4.1.10 Recommendation 10 - Prince2 and PMBOK

Recommendations received: 2

Participants requested emphasis on project management over prescribing adoption of Prince2, again emphasising that practicability is preferred over rigidity. One participant also pointed out that the quoted Prince2 release date was incorrect.

#### 7.4.1.11 Recommendation 11 – TOGAF

Recommendations received: 8

Most of the participants commented on this recommendation. There was a request to contextualise the use of cloud computing in the framework and update some of the references. A number of participants felt that there was too much emphasis on adopting TOGAF, considering the multitude of architecture tools and frameworks.

#### 7.4.1.12 Recommendation 12 – VALIT

Recommendations received: 1

Participants were generally unaware of ValIT and some questioned its inclusion. Experience has shown value management to arguably be the most complex, worst-structured aspect of IT governance, so some guidance is required and nothing substantial exists apart from ValIT, which has, since the interviews, been integrated with COBIT 5.

#### *7.4.1.13Recommendation 13 – King III Report*

Recommendations received: 7

Participants emphasised the importance of the compliance function, including how the IT reporting requirements to the Board should be met. Participants asked for more detailed guidance on how the Board reporting for IT should be dealt with. Contextualising King III conformance against the total combined assurance concept was also highlighted as a requirement. Listed companies and some of the larger organs of State have devoted significant resources and time to the improvement of IT governance, following the publication of King III, so any South African IT governance project should be measured against the requirements of KingIII, Chapter Five, which deals with IT governance. The large number of participant comments on this recommendation confirm this.

#### *7.4.1.14Recommendation 14 – ISO/IEC38500*

Recommendations received: 5

Recommendation 6 dealt with comment related to ISO/IEC38500.

#### *7.4.1.15Recommendation 15 – IT Sub Processes*

Recommendations received: 1

One participant requested clarification on the meaning of "sub processes".

#### *7.4.1.16Recommendation 16 – IT Control Framework*

Recommendations received: 0

All participants agreed with the recommendation, as the kind of organisations participating are likely to have a more mature control environment, with more formal systems of internal control.

#### *7.4.1.17Recommendation 17 – Supporting Documents*

Recommendations received: 0

All participants agreed with the recommendation. Again, the likely control maturity of participating organisatons is reflected in their understanding and agreement with this recommendation.

#### *7.4.1.18Recommendation 18 – Architecture*

Recommendations received: 5

Refer to Recommendation 11, where being prescriptive on the adoption of TOGAF was dealt with. There was alo a request to contextualise the security architecture, which is a pervasive aspect of the internal control environment.

#### *7.4.1.19Recommendation 19 – Portfolio Management*

Recommendations received: 1

The single comment received here duplicated aspects of the value management comment, which was dealt with under Recommendation 2.

#### *7.4.1.20 Recommendation 20 – Desirable Practices Conclusion*

Recommendations received: 1

One participant pointed out that the table supporting the recommendation lacked colums for ValIT, RiskIT, ISO/IEC20000 and ISO9001. It was also noted that Prince2 and PMBOK had not been indicated as practices supporting Risk Management.

#### *7.4.1.21 Recommendation 21 – Office of the CIO*

Recommendations received: 2

Comment related to the need for clarity around roles was dealt with under the general section above.

#### *7.4.1.22 Recommendation 22 – Chief Technology Officer*

Recommendations received: 1

One participant requested that the framework emphasise how the CTO role could become more prominent in future because the CIO role is becoming less technical and more business focused. Very few South African organisations have a true CTO role and there is no general agreement on the definition of the role.

#### *7.4.1.23 Recommendation 23 – Information Security Officer*

Recommendations received: 4

Participants requested a balance of the general practice of having the ISO role inside IT with the ideal position of it being a business function. Pragmatism is important to finding a practicable solution. Like the enterprise architecture function, the skills for this role generally do not exist in business, which is the reason for this often becoming a delegated IT responsibility.

#### *7.4.1.24 Recommendation 24 – Technology Architect*

Recommendations received: 2

A few participants requested clarification about which architecture roles should be inside and which outside IT. This is important, as most of the layers of enterprise architecture should ideally reside outside IT, although, in practice, most architecture activity takes place inside IT. Again pragmatism is important.

#### *7.4.1.25 Recommendation 25 – IT Financial Manager*

Recommendations received: 0

All participants agreed to the recommendation.

#### *7.4.1.26 Recommendation 26 – IT Risk Officer*

Recommendations received: 3

As mentioned earlier, participants see IT risk management as an important sub set of ERM that cannot exist separately. Some participants highlighted the need for a more comprehensive IT governance role that incorporates the responsibility for IT risk management and monitoring the effectiveness of internal IT controls. As such, the expectation also exists that this person should continually report on IT risk management and control effectiveness. This makes sense in the context of the growing governance, risk, control and compliance awareness, and would fit well into the combined assurance function.

#### *7.4.1.27 Recommendation 27 – Applications Manager*

Recommendations received: 2

Some participats felt the need to elaborate on the recommendation related to the applications manager role, as well as the segregation of environments, that is development from testing and production, and development roles from support roles. Segregation is a key control concept and highly important to effective IT governance.

#### *7.4.1.28 Recommendation 28 – Technical Manager*

Recommendations received: 2

Two participants suggested that the responsibility for infrastructure projects be assigned to the technical management role. This makes sense, as this role understands the existing infrastructure and would be well positioned to oversee infrastructure projects.

#### *7.4.1.29 Recommendation 29 – Operations Manager*

Recommendations received: 0

All participants agreed to the recommendation.

#### *7.4.1.30 Recommendation 30 – IT Strategy Committee*

Recommendations received: 1

Recommend combination of IT Strategy and Steering Committees.

The detailed questionnaire confirmed that almost all of the participants prefer a combined rather than separate committee, so only one person felt it necessary to comment on this again.

#### *7.4.1.31 Recommendation 31 – IT Steering Committee*

Recommendations received: 3

As the participants in the IT Steering Committee and IT Strategy Committee are largely the same, participants requested the positioning of the option of having one body with two distinct agendas. A further distinction was suggested between the Executive and IT Steering Committee in this regard as, in practice, the IT Steering Committee is almost exclusively composed of Executive Committee (EXCO) members.

#### *7.4.1.32 Recommendation 32 – Technology Architecture Forum*

Recommendations received: 7

Most participants responded to this recommendation, including requesting architectural oversight over the IT architecture, clarifying where the information security officer role should be situated and adding a definition of the extended enterprise.

#### 7.4.1.33 Recommendation 33 – Programme Management Office

Recommendations received: 1

One participant suggested that the framework explain that the PMO structure depends on the organisational culture. This is true, as governance styles depend on and should be styled in line with culture.

#### 7.4.1.34 Recommendation 34 – IT Governance Roles

Recommendations received: 4

Participants requested additional detail related to the roles of the service manager, the EXCO's responsibility for IT governance, and roles responsible for resource and performance management, as far as people are concerned.

#### 7.4.1.35 Recommendation 35 – IT Governance Structures

Recommendations received: 5

Paticipants requested greater clarity related to architecture, as far as it concerns IT architecture, so the business responsibility for the other architecture layers is not diluted. They further suggested an update of the PES cube to include the Board. The research interviews started prior to the publication of King III. Chapter Five of King III emphasises the accountability of the Board for IT governance, so this would be a key omission, unless addressed. Similarly, their expectation was for the framework to clearly state the EXCO's delegated responsibility for effective IT governance, as opposed to the Board's accountability. Under King III, the CIO has a delegated responsibility towards the EXCO for discharging practical IT governance responsibilities. The framework needs to reflect these delegated accountabilities. Exco's responsibilities are reflected under the IT Steering Committee column, as EXCO would contribute most members of the IT Steering Committee.

## 7.5 Questionnaire Analysis Summary

Participants' comment came in the form of non-structured feedback and a detailed questionnaire to determine their views on specific aspects of the framework in a more structured manner.

The structured feedback, which has been summarised in sections A through F below, is depicted by a full set of graphs, which are included in Appendix Two (Graphs Suporting Analysis). For each question, a graphic depiction is provided, whether the question was accepted, considered or not accepted, deductions made from the feedback, and a cross-reference to the recommendations they support. A summary of the analysis of the graphs in the appendix follows.

### 7.5.1 A. General

The concept of the Office of the CIO is highly important or critical to effective IT governance. The Office depends on the clarity of its supporting roles.

The IT financial manager, IT risk officer, service support manager and service delivery manager roles are of significant importance and warrant full-time appointments. In addition, the roles of applications manager and IT operations manager are of significant importance. The technical manager role could be combined with other roles without compromising its effectiveness. The preferred reporting line for the service support manager is to the operations manager.

The IT operational model depends on and should follow the culture of the organisation. Vendor management is significantly important to the PES IT Governance Framework. IT procurement should be part of the corporate procurement process, which could be centralised or federated, depending on the organisation. Depending on the organisation, the Procurement function might handle all aspects of IT procurement and IT vendor management.

An IT Steering Committee is a significantly important part of effective IT governance. Organisations prefer to combine the IT Strategy Committee and IT Steering Committee.

The CTO role is useful but not of high importance. Consequently, it is not highly important to segregate the CIO and CTO roles.

It is of significant importance to implement the IT governance chapter of King III. The formal take up of ISO/IEC38500 has been low and it is not highly important to implement the standard, yet it plays a significant part in COBIT 5 and has been incorporated into some implementations of King III.

### 7.5.2 B. Strategic Alignment

IT strategy should be updated at least annually, with consideration given to an update midway through the year.

The business architecture belongs to business, while the remaining architecture layers belong to the IT function. Enterprise architecture should be closely linked to the corporate strategy function, to translate strategy into action.

For the purposes of the PES IT Governance Framework, the IT architect role should be emphasised above the enterprise architect role. Similarly, the Technology Architecture Forum should be emphasised above the Enterprise Architecture Forum. Enterprise architecture framework adoption should not be limited to TOGAF, as a variety of architecture standards, methods and tools are available. IT architecture should be an IT responsibility, but business should be responsible for the other layers of the enterprise architecture.

It is important to align IT services to the IT strategy on an ongoing basis. Integration between corporate strategy and enterprise architecture is of significant importance. This suggests that integration of IT strategy and IT architecture is also significantly important.

### 7.5.3 C. Value Delivery

An EPMO with responsibility for handling IT projects is of importance. It is imperative to incorporate the IT PMO into the IT governance structures, regardless of whether this is a standalone PMO or part of the EPMO. Adoption of a formal project management methodology and service level management is significantly important to sound value delivery. The governance over projects is more important than adopting Prince2 or PMBOK. IT portfolio management is of importance to enterprise portfolio management. IT service portfolio management is significantly important for the continual alignment of IT services to business needs.

### 7.5.4 D. Resource Management

It is of importance to IT to adhere to corporate resource management processes. Utilising ITIL is significantly important to practising sound IT governance, including implementing formal service support and delivery, together with a dedicated help desk or service desk to facilitate effective IT service management. Implementing formal software asset management is of importance to practising sound IT governance.

### 7.5.5 E. Risk Management

Integrating IT risk management and operational risk management is significantly important to sound IT risk management. An ERM representative inside IT should be responsible for management of IT risk, as part of ERM. Having formally identified, categorised and classified information assets is of significant importance. Performing annual IT risk assessments, with six-monthly follow-up is of significant importance.

Having a formal information security management function, that is segregated from IT is of significant importance. The information security manager role is important, but it does not detract from the effectiveness of the role if it is situated inside the IT organisation. It is not significantly important to have a full-time information security officer.

It is of importance to base information security management on ISO/IEC27000. Basing the IT control environment on COBIT is important. It is significantly important to implement a formal IT control framework. It is of significant importance to formalise IT processes, policies, procedures and standards. Monitoring the development of Risk IT is of significant importance.

### 7.5.6 F. Performance Measurement

IT performance management is important, regardless of whether a balanced scorecard is implemented or not. The aggregated responses have been analysed and a summary of participant input provided below, per recommendation and practice preference, in order to inform what should be included in the final version of the proposed IT governance framework.

### 7.5.7 Aggregated Results

| | **Practice recommendations** | | **Binary practice evaluations** | | **Multiple practice evaluations** | |
|---|---|---|---|---|---|---|
| | **Number** | **Percentage** | **Number** | **Percentage** | **Number** | **Percentage** |
| Accepted | 36 | 73% | 5 | 71% | 5 | 24% |
| Considered | 12 | 24% | | | 2 | 10% |
| Not accepted | 1 | 2% | 0 | 0% | 14 | 67% |
| Undecided | | | 2 | 29% | | |
| | ***49*** | ***100%*** | ***7*** | ***100%*** | ***21*** | ***100%*** |

**Table 7.1 – Questionnaire Results Summary**

Almost all practice recommendations were accepted or at least considered. Only one (two %) of these recommendations was flagged as *not accepted.* This related to the question on the importance of, "having a formally assigned IT security officer role, allocated to a person outside IT", where four respondents chose *somewhat important* and two *not important.* This could be ascribed to the real-world practice where the role is situated inside IT rather than in business, currently being more practicable than the theoretical option.

None of the binary option practice recommendations were not accepted, but in 29% of the cases, participants could not decide between proposed practices. The multiple practice evaluation questions tested combinations of possibilities and were successful in eliminating two thirds of the options to arrive at a clearer set of preferences for inclusion in the framework. Table 7.1 is presented in the form of three pie charts below.

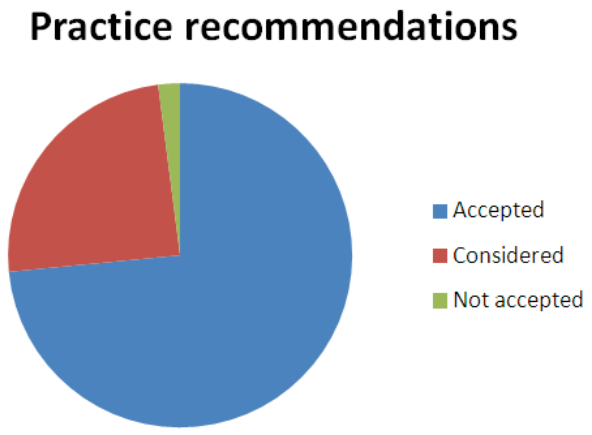


**Diagram 7.1 – Classification of practice recommendations**

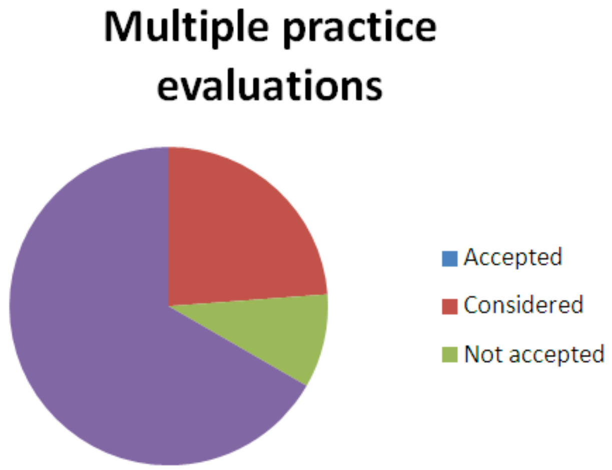


**Diagram 7.2 – Classification of multiple practice evaluations**

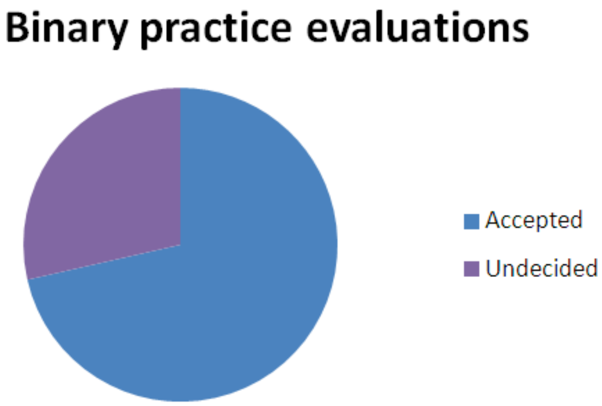


**Diagram 7.3 – Classification of binary practice evaluations**

For further reference, Appendix Three contains the raw data behind the questionnaires, with a cross-reference to the recommendations in the proposed IT governance framework.

## 7.6 Conclusion

Participants have commented on the PES IT Governance Framework in detail, which was reinforced by clear selections of options presented in the questionnaire. The Framework was largely accepted as presented, with indications by participants as to what they disagree with or would like presented in a different way. The widest varying input was around the practices to be adopted for implementing the Framework. Other changes flowing from this will largely be to make certain roles and structures more IT specific, for example around architecture, and to include aspects that were completely omitted from the initial framework, such as the role of the Board and COBIT 5. Participant input was successfully collected and analysed, to serve as the basis for a more practicable IT governance framework.

# Chapter Eight: Final Amended Framework

## 8.1 Abstract

Chapter Seven presented an analysis of the results of the empirical work. This chapter presents amendments to the proposed PES IT Governance Framework, based on the results of the empirical work, to produce a final, amended PES IT Governance Framework.

## 8.2 Introduction

### 8.2.1 Background

In a world of continually increasing regulatory pressure, a long history of poor corporate governance and shareholder activism, IT governance has gained prominence to the extent where The King Report on Governance for South Africa 2009 (King III) devoted an entire chapter to the topic. King recommends the implementation of an IT governance framework, but finding a generally applicable framework has proven to be a challenge that has not yet been addressed. COBIT 5 was expected to substantially address this problem, but at this stage, there is still much debate as to how exactly the new release should be applied.

This document presents a generic IT governance framework, based on a literature review and input by ten CIOs of large South African organisations, with annual revenue in excess of R1bn for private sector companies or a budget in excess of R1bn in the case of government organisations.

Diagram 8.1 of the proposed PES IT Governance Framework below is repeated from chapter five.

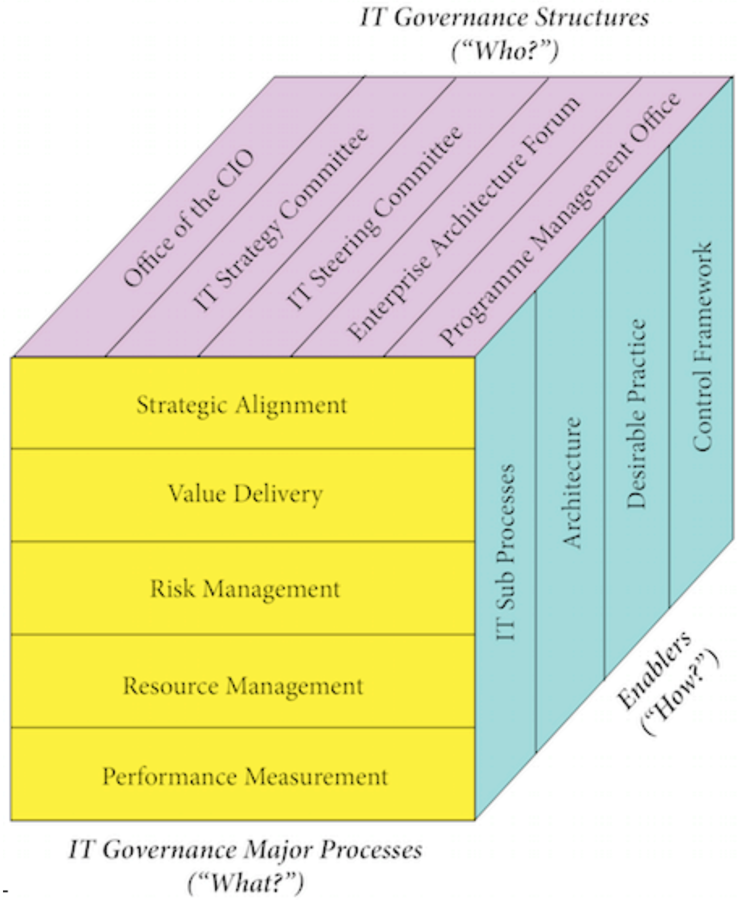


**Diagram 8.1 – Original PES IT Governance Framework**

The definition of an IT governance framework adopted for this research is, "the underlying structure supporting IT governance through the combination of governance structures, architecture, processes, desirable practices and an IT control framework to effectively support the IT governance major processes".

According to this definition, the components making up the "underlying structure" or framework are:

i) Processes: The five IT governance major processes are broken down into sub processes, modelling all aspects of the IT environment. Governance structures, desirable practices and IT controls map back to the major processes, while the processes map back to the enterprise architecture;

ii) Governance structures: These are the roles, positions, governing bodies and structures overseeing IT governance in the organisation;

iii) Architecture: The IT component (IT architecture) of the enterprise architecture, which reflects the composition of the organisation and the alignment of all architectural elements to organisational objectives;

iv) Desirable practices: The definition formulated in the Introduction to this dissertation is, "the most appropriate practice accepted by consensus as a de facto standard or through certification as a de jure standard". More specifically, this research takes an interest in desirable practices supporting IT governance; and

v) IT control framework: In the Introduction to the dissertation from which this framework was derived, the definition provided was "the underlying structure of the IT internal control environment, including all the most significant (or key) controls for the IT environment, together with the complementary, supporting (or non key) controls".

To facilitate a structured, logical approach to constructing a generic framework, the researcher summarised the five components mentioned above into the three dimensions of the original PES Framework, presented in diagram 8.1, namely:

- The IT governance major processes, as mentioned earlier, represent the high-level processes that form the backbone of the framework and are used as the focal integration point of the IT governance framework. The major processes specify what should be done to practise sound IT governance, more specifically IT risk management, performance management, strategic alignment, resource management and performance management;
- Enablers for IT governance, which are the embodiment of day-to-day IT governance and specify how sound IT governance should be practised; and
- The roles and structures for effective IT governance are the main roles and bodies for effective IT governance. The IT governance structures specify who all are responsible and accountable for the effectiveness of the sub processes making up the five IT governance major processes.

### 8.2.2 Objectives

The objectives of the research were to validate and amend a proposed draft framework, presented to the ten CIOs, to arrive at a generic IT governance framework that is relevant to all the organisations interviewed, and identify IT governance trends across the organisation interviewed.

*(Note: To enable the reader to identify changes between the original and final, amended frameworks, significant changes between the two are italicised below.)*

### 8.2.3 Final, Amended PES IT Governance Framework

Diagram 8.2 below presents the final, amended PES IT Governance Framework.

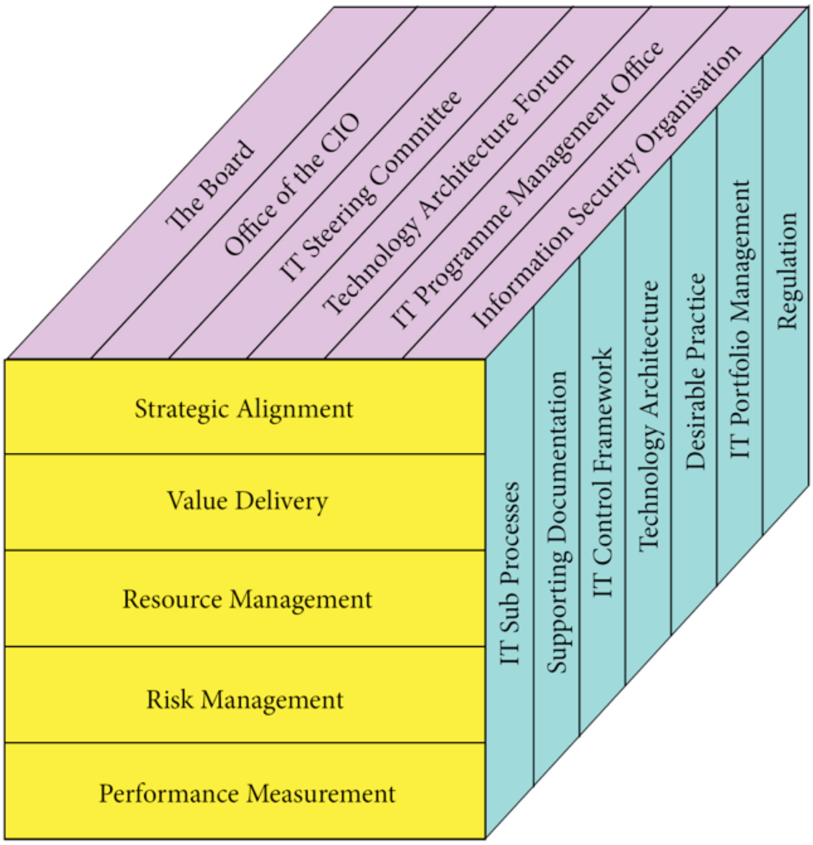


**Diagram 8.2 – Final, Amended PES IT Governance Framework**

*The amended PES IT Governance Framework depicted in diagram 8.2 provides a single, cohesive view that could be populated to serve as a generic framework suitable for any large IT organisation. This document is structured around the three dimensions of the cube and covers all of its components below. The differences from the originally proposed framework (diagram 8.1) to the amended PES IT Governance Framework (diagram 8.2) are visible in the IT Governance Structures ("who") and Enablers ("how") dimensions. A key omission from diagram 8.1 was the role of the Board. Input from the participating CIOs suggested that the IT Strategy Committee should not exist apart from the IT Steering Committee and that information security should be given more prominence. To improve the focus on IT governance, participants indicated that the Enterprise Architecture Forum should be replaced with the Technology Architecture Forum, the Programme Management Office with the IT Programme Management Office, Architecture with Technology Architecture, and the Control Framework with an IT Control Framework. The participants also highlighted that the ever-increasing compliance pressures neccesitate the inclusion of regulations, the importance of policies require the inclusion of supporting document,s and true IT governance relies heavily on IT portfolio management.*

## 8.3 IT Governance Major Process Recommendations

The proposed structures and enablers should all be viewed in the context of the five major processes, which are described below.

### 8.3.1 Strategic Alignment – Recommendation 1

Strategic alignment requires IT objectives (and accordingly the IT strategy), IT operations and investment in IT to support the achievement of organisational objectives. In its most basic form, strategic alignment of IT to organisational objectives starts with IT strategic planning.

Enterprise architecture and IT portfolio management provide valuable mechanisms for aligning IT to business; enterprise architecture is considered as a means of ensuring that structures, processes, systems and infrastructure are aligned to organisational objectives; IT portfolio management is considered to support the alignment of IT projects and services to organisational objectives.

Bodies involved in monitoring the strategic alignment of IT include the Enterprise Architecture Forum, the IT Strategy Committee and IT Steering Committee.

In the IT context, sound governance requires the alignment of IT strategy, planning, investment and operations to technologically enable departments contributing to strategic objectives. This is achieved by implementing a performance management process, which includes the formulation of IT objectives with related KPIs that make it clear how IT would enable these departments to achieve their objectives.

#### *8.3.1.1 Implementation Guidance*

- Organisations should have a formal IT strategy that is aligned to organisational objectives and that is updated at least annually, if not twice a year;
- IT services should be aligned to the business strategy, either informally or through non-business architectural layers and service portfolio management mechanisms;
- *Business should prioritise strategic IT requirements;*
- *Architecture* and IT portfolio management should be considered as mechanisms for aligning IT and organisational strategies;
- *An IT Steering Committee, incorporating IT strategy responsibilities,* should be instituted to oversee the alignment of the IT strategy to the organisational strategy;
- *In federated IT organisations, distributed IT entities should be aligned across the organisation;*
- *The IT strategic alignment process should be formalised, with a change management process to embed organisational changes that might be necessary to enforce more sustainable practices and structures;*

- *The establishment of architecture forums for application, information and technical architecture layers should be considered, with IT being responsible for alignment of the technical architecture layer to the other layers.*

### 8.3.2 Value Delivery – Recommendation 2

The focus of value delivery is often on ROI, that is, does the investment in IT yield the return expected at the point of committing to the investment? Value management extends beyond this question and should adequately address benefits realisation, risk optimisation and resource optimisation as its key focus areas.

An important mechanism for managing value delivery is the service level management process, which manages and monitors service delivery in accordance with the service strategy and design. Service level management is a service delivery process, included in the IT Infrastructure Library (ITIL). As a vehicle for facilitating value delivery, the IT PMO is a structure that translates IT strategy into execution. Where IT organisations are most successful at delivering value, IT governance practices are often embedded within broader corporate governance. This manifests in areas like IT portfolio management, where the enterprise and IT processes are aligned or formally integrated. Sometimes overlooked as a value delivery enabler, enterprise architectural competency presents a critical part of value delivery.

#### *8.3.2.1 Implementation Guidance*

- The service level management process should be formalised to closely monitor value delivery at the operational level;
- A PMO should be established to monitor significant IT projects or, as appropriate, multiple PMOs;
- *PMO responsibilities should be aligned to business structures and segregated from project delivery responsibilities;*
- The role of enterprise architecture should be considered as an enabler of value delivery;
- *The COBIT5 value management processes that were derived from ValIT should be embedded, particularly those dealing with benefits formulation, monitoring and reporting;*
- *The value debate should cover the strategic impact of not investing at the appropriate time on strategy execution.*

### 8.3.3 Resource Management – Recommendation 3

IT resourcing includes people, processes, systems (applications, data, information and infrastructure), and finances.

Formal IT processes are required to manage these resources and are supported by policies, procedures, standards, methodologies and an internal IT control framework. To formalise IT processes, the desirable practices discussed in the Enablement section should be applied.

Specific enablers supporting resource management are IT service management, IT project management (monitored via an IT PMO), and information security management. The management roles identified in the IT Governance Structures section are the ones responsible for resource management.

#### *8.3.3.1 Implementation Guidance*

- The official organisational processes for managing people, systems, information, infrastructure, energy, and finances should be practised in IT, and that specific processes be implemented for IT service management, IT project management (monitored via a PMO) and information security management.

- *Where services are outsourced, the emphasis should be on vendor management and managing service quality through the service level management process.*

- *Consider how business intelligence could be applied to support the monitoring of resource management and performance measurement.*

- *Active vendor management should become more prominent in IT.*

- *The recommended roles are important, even where they cannot be entertained in individual positions, but instead have to be assigned in combined roles.*

### 8.3.4 Risk Management – Recommendation 4

IT risk management focuses on three processes, namely Risk Governance, Risk Evaluation and Risk Response, in order to:

- Set responsibility for IT risk management;
- Set objectives and define risk appetite and tolerance;
- Identify, analyse and describe risk;
- Monitor risk exposure;
- Treat IT risk; and
- Link with existing guidance to manage risk.

RiskIT was the IT Governance Institute's first step in establishing a formal directive on IT risk management, as a complementary publication to COBIT 4.1 and ValIT. RiskIT provided an initial mapping between COBIT 4.1 and the IT risk management process. With the release of COBIT 5, RiskIT was incorporated into COBIT.

The traditional view of IT risk management has often emphasised information security management and IT service continuity management. When comparing RiskIT, ITIL (specifically the IT Service Continuity Management Process) and ISO/IEC27001 (Information Security Management Process) it becomes clear that more or less the same process could be followed for identifying and analysing risk pertaining to any aspect of IT.

Some IT risk management programmes are not aligned to enterprise risk management. Effective IT risk management is only possible as a sub set of the overall enterprise risk management process. Conversely, all line managers who rely on IT should contribute to IT risk management.

#### *8.3.4.1 Implementation Guidance*

- A formal IT risk identification and assessment process should be implemented, as well as a formal IT control framework indicating the approved responses to all significant IT risks.

- The RiskIT processes, which were embedded in COBIT5, should be considered to formalise IT risk management.

- IT risk management should be integrated into the enterprise risk management process and should be part of an overall combined assurance process.

### 8.3.5 Performance Measurement – Recommendation 5

Performance measurement monitors strategy implementation, project completion, resource usage, process performance, and service delivery. Balanced scorecards monitor the translation of strategy into action. The IT Governance Institute proposes the implementation of an IT balanced scorecard incorporating the following perspectives:

- Enterprise contribution – How do business executives view IT?

- User orientation – How do users view IT?

- Operational excellence – How effective and efficient are the IT processes?

- Future orientation – How well is IT positioned to meet future needs?

#### *8.3.5.1 Implementation Guidance*

- The IT performance measurement process should be implemented to monitor operational and tactical performance, whether in balanced scorecard fashion or using any other proven method.
- *IT performance management should be aligned to corporate performance management.*

- *IT performance management should include communication of corporate and IT strategy, so performance management objectives are understood clearly.*

## 8.4 Enabler Overview

The proposed enablers required to implement a generic IT governance framework are described below.  It is important to note that these enablers are not presented based on their perceived importance.

### 8.4.1 ITIL – Recommendation 6

ITIL represents desirable practice for Service Management and the complete service lifecycle, from service strategy through to service operation, including all aspects of service support and service delivery.

The Global Status Report on the Governance of Enterprise IT – 2011, issued by the IT Governance Institute, shows that ITIL is considered the most referenced practice influencing IT governance frameworks.

Prior to the ITIL 3 and the latest revision called ITIL 2011, the most widely known ITIL publications were the Service Support and Service Delivery modules, which cover the following processes:

- Service Support: Configuration management, change management, release management, incident management, problem management, and the service desk function.
- Service Delivery: Service level management, financial management for IT services, capacity management, IT service continuity management, and availability management.

In ITIL 2011, the Service Support and Service Delivery publications were not replaced, but incorporated into the Service Capability modules, namely:

- Planning, Protection and Optimisation;
- Service Offerings and Agreements;
- Release Control and Validation; and
- Operational Support and Analysis.

Five lifecycle modules were introduced:

i) Service Strategy;
ii) Service Design;
iii) Service Transition;
iv) Service Operation; and
v) Continual Service Improvement.

ISO/IEC20000, the international IT Service Management standard, has not yet been implemented widely in South Africa. Organisations have instead focused on implementing prioritised aspects of ITIL.

#### *8.4.1.1 Implementation guidance*

ITIL or a branded version of it, such as the former Microsoft Operations Framework should be used when formulating IT service strategy, design, operation and general IT service management processes, implementing a security management system as described by ISO/IEC27000 or when designing IT/ business alignment mechanisms.

The IT service management standard, ISO/IEC20000 is only recommended for organisations striving to achieve international ITIL certification. It does not directly support the proposed IT governance framework.

### 8.4.2 COBIT – Recommendation 7

Since its birth in the late 1990s COBIT has, at the time this research was conducted, matured into COBIT 5. According to the Global Status Report on the Governance of Enterprise IT – 2011, COBIT 4.1 was the fourth most referenced among frameworks considered to be influencing IT governance. RiskIT was listed two positions below COBIT 4.1, while ValIT held 12th position. Since the report was issued, COBIT 5 was released, which now incorporates aspects of COBIT 4.1, RiskIT, ValIT and the Business Model for Information Security (BMIS), which was listed in 10th position in the 2011 report. One might therefore expect COBIT 5 to achieve a higher ranking, should another Global Status Report on the Governance of Enterprise IT be released. COBIT 5 marks a clear departure from its predecessors, which had all been focused primarily on a set of control objectives that traditionally supported the audit profession.

COBIT4.1, still the most widely used publication in the COBIT family, adopts a generic view of the IT environment, breaking it down into 34 processes that are grouped into the four domains of Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. Each of the 34 processes is broken down into control objectives that are classified according to resource types impacted (applications, information, infrastructure or people), business requirements (effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability), and IT governance major processes impacted. To facilitate formal process design, each process also has a suggested list of inputs from and outputs into other processes, a RACI chart summarising responsibilities and accountabilities for roles related to the process, goals and metrics, and suggested maturity ratings.

At the time this research was concluded, the COBIT 5 family included COBIT 5, COBIT 5: Enabling Processes, COBIT 5 Enabling Information, COBIT 5 Implementation, COBIT 5 for Information Security, COBIT 5 for Assurance, COBIT Assessment Programme and COBIT 5 for Risk. COBIT 5 has positioned itself strongly as an enterprise governance framework serving the business, rather than a set of control objectives serving the IT auditing community, as it had been doing up to COBIT 4.1. At this stage, South African organisations are still coming to terms with aspects of King III's IT governance requirements and it would appear that the business community has not yet taken notice of COBIIT 5. Instead, the traditional auditing users have made more of an effort to understand the new products and their application, though they have not yet agreed exactly how COBIT 5 for Assurance will support the audit process, that is how the inferred (indirect) control objectives, embedded in the Process Reference Model (COBIT 5: Enabling Processes), will be applied.

It also remains to be seen how the traditional users of ISO/IEC27000 will be convinced to use COBIT 5 for Information Security, considering the substantial investment some organisations have already made in ISO/IEC27000-based products. For the purposes of the proposed IT governance framework recommended by this paper, the recommendation would be that organisations focus on applying the process reference model when implementing or improving IT governance processes or the processes supported by the recommended practices. The ValIT Framework, originally published by the IT Governance Institute during 2006, provided a useful structure for value delivery, comprising value governance, portfolio management and investment management. ValIT was a unique and valuable publication, yet very few organisations adopted it. Like RiskIT, COBIT 5 incorporates ValIT, making it a more comprehensive IT governance publication.

#### *8.4.2.1 Implementation Guidance*

- For companies that adopt COBIT 4.1 or COBIT 5, it is recommended that the processes which the practice propose be prioritised and that the following be done for each selected high priority process:
  - A procedure be adopted to serve as the minimum level of formalisation of the process and as the basis for a consistent approach to the process;
  - Where possible, desirable practice be followed to implement the procedure;
  - Key controls be defined and implemented for the process, and staff trained on the effective use of each control; and
  - Input from internal and external audit sought on the design effectiveness of key controls.
- *In the case of COBIT 4.1, process maturity targets should be established, using the CMMI grading included per COBIT 4.1 process.*
- *Where COBIT5 is adopted, process capability targets should be established, based on the COBIT5 Process Capability Model.*
- *The ValIT processes that were taken into COBIT5 should be considered to formalise value management.*

### 8.4.3 The ISO/IEC27000 Family of Standards – Recommendation 8

The ISO/IEC27000 series currently includes ISO/IEC27001, which specifies the requirements for establishing an information security management system and 27002, which has absorbed ISO/IEC17799. In its third version, ITIL now provides guidance on the security management process, as it relates to all other operational IT processes. As such, ITIL V3 is an important complement to ISO/IEC17799 and ISO/IEC27001 for managing information security. The ITIL Information Security Management Process provides a security framework, information security policy and guidance for implementation of the ISO/IEC17799 security management system.

#### *8.4.3.1 Implementation Guidance*

- *Organisations striving for more mature information security management processes should consider formally implementing an ISO/IEC27000-based information security management system.*
- *ITIL supports access management and aspects of the security management system promoted by ISO/IEC27000, and should be considered as a minimum for organisations choosing not to implement ISO/IEC27000.*
- *The ISO/IEC27000 family is comprehensive and necessitates careful consideration of the appropriate sub standards supporting the organisation's objectives, rather than expecting to implement all aspects of the standard.*

### 8.4.4 Balanced Scorecard – Recommendation 9

In the early nineties Robert Kaplan and David Norton coined the term, "balanced scorecard" (Kaplan, 1996:viii), a term that has since become widely used in corporate performance measurement circles. "The Balanced Scorecard provides executives with a comprehensive framework that translates a company's vision and strategy into a coherent set of performance measures (Kaplan 1996:24)." The balanced scorecard is "a carefully selected set of quantifiable measures derived from an organisation's strategy" (Niven, 2006:13). Many variants of the original balanced scorecard exist but are all based on the initial concepts articulated by Norton and Kaplan (Olve, 2006:15). The balanced scorecard provides an effective framework for implementing governance communications, based on its focus on strategic alignment, its perspective beyond financial measures, and its combination of leading and lagging metrics (Symonds, 2009:4).

#### *8.4.4.1 Implementation Guidance*

- IT organisations should implement an IT performance measurement mechanism, for example a balanced scorecard, to address the performance measurement process in the generic framework.
- *The selected mechanism should form part of the IT reporting framework.*
- *Metrics should also cover IT value generation or benefits realisation and compliance to appropriate standards, legislation and regulation.*

### 8.4.5 Prince2 and PMBOK – Recommendation 10

Prince2 provides a structured method for effective project management, whereas PMBOK is the definitive work on project management standards. As such, it complements PMBOK, providing the "how" while PMBOK states the "what". The current edition of Prince2 was released in 2009. Prince2 defines a project management method, providing a framework for the wide variety of project disciplines and activities. Prince2 focuses on the business case, which drives all project management processes, from initiation to conclusion. Considering the findings of the Global Status Report on the Governance of Enterprise IT – 2011, PMBOK and Prince2 are considered project management-related desirable practice. The Project Management Institute publishes PMBOK, which provides general guidance on all aspects of project management, including integration, scope, time, cost, quality, human resources, communication, risk, and procurement management. Prince2 provides a structured method for effective project management, namely meeting the standard defined by PMBOK.

#### *8.4.5.1 Implementation Guidance*

- As the definitive work on project management, it is recommended that PMBOK should be used as the project management standard for organisations adopting the generic IT governance framework, with a project management method such as Prince2 for comprehensive project management processes.
- Organisations have a number of project management methods, so any structured method could be used if Prince2 or PMBOK are not formally adopted.

### 8.4.6 TOGAF – Recommendation 11

The Open Group Architecture Framework provides a generic enterprise architectural framework to a wide community in a similar way the Open Source Movement supports sharing of software. In its list of frameworks influencing IT governance, the Global Status Report on the Governance of Enterprise IT – 2011 (IT Governance Institute, 2011:29) included TOGAF as the only considered architecture framework. Even though it was only adopted by 2.9% of the organisations it was the only architecture framework regarded as significant enough for inclusion and, according to the Status Report, remains one of the two most-cited IT-related certifications, alongside Prince2. With the increasing number of publications such as ITIL advocating a services orientation, organisations might do well to consider the suitability of adopting a service-oriented architecture, which makes services available in a transparent manner. Enterprise architecture aspects, as far as the roles of the chief enterprise architect and Enterprise Architecture Forum are concerned, are discussed in the IT Governance Structures section.

#### 8.4.6.1 Implementation Guidance

- Organisations should explore ways of formalising their enterprise architectures through the use of architectural frameworks like TOGAF and the work of Weill and Ross.
- It is important to understand that architecture is a means to support the strategic alignment major process, rather than being an end in itself.

*(Note – in the original framework, recommendation 12 dealt with ValIT, which has since been integrated with COBIT 5. Participants emphasised the importance of compliance and regulatory requirements, which have, in this update, been incorporated under recommendation 12.)*

### 8.4.7 Regulatory Requirements and Sarbanes-Oxley – Recommendation 12

*Recommendation 12 was previously formulated around ValIT, which has, since the original framework, been incorporated into COBIT 5. In addition, the proposed framework did not address regulatory requirements, so to maintain the structure, provision was made for ValIT in the COBIT-specific recommendations (refer Recommendation 7), while Recommendation 12 is now focused on regulatory requiremens, including those for Sarbanes-Oxley, as suggested by some participants.*

*New regulatory requirements are being introduced continually. One of the most rigorous to conform with is the Sarbanes-Oxley Act of 2002 (SOX), which is US legislation applicable to listed company boards, management and public accounting firms. Section 404 deals with the assessment of internal control and focuses an IT governance programme on implementing an effective internal control framework (refer 4.11 below). Listed US companies and their significant operations in other countries need to be able to prove that they had effective IT controls throughout the financial year in support of applications involved in the production of financial statements and key financial management reports. Control effectiveness implies both design and operating effectiveness.*

#### 8.4.7.1 Implementation Guidance

- *All organisations should be aware of regulatory developments and their requirements of the IT function. Companies that are listed in the US should implement the following for applications that are in-scope, due to them supporting key statutory controls:*
- *Formalise key IT general and application controls;*
- *Implement the necessary self-assessment processes for IT;*
- *Maintain evidence proving the effective operation of key IT controls on an ongoing basis; and*
- *Institute a continual improvement process to remediate defective controls shown by self-assessments, internal and external controls.*

### 8.4.8 King III Report – Recommendation 13

The past few years have seen some significant publications that no listed South African company or government organisation can ignore in its approach to practising IT governance. The King Report on

Governance for South Africa 2009 ("King III") has become an important requirement for the larger players in corporate South Africa, while over the longer term, the first international standard on IT governance, COBIT 5 and ISO/IEC38500, might become the global reference works on IT governance fundamentals.

Any generally accepted, generic South African IT governance framework will have to incorporate the principles of these publications in order to ensure its long-term relevance. King III is relevant to all South African companies, particularly those listed on the Johannesburg Stock Exchange. New listing requirements and potential future corporate financial reporting standards are expected to contain a statement of conformance to King III, which now includes a section dedicated to IT governance.

#### *8.4.8.1 Implementation Guidance*

Where the organisation has decided to implement the recommendations of the King III report, it is recommended that the following be implemented to fulfil the requirements of the IT governance chapter of King III:

- A Board IT governance awareness programme should be undertaken to ensure the directors understand all aspects of IT governance, for which they are accountable.
- An IT charter should be established, setting out the objectives of the IT function in support of organisational objectives, including sustainability objectives, and governance requirements of the IT function. The charter should also define all key IT governance structures and roles, and their decision-making responsibilities and accountabilities.
- A set of policies, procedures and standards should be implemented to guide behaviour in IT, in line with the IT charter.
- As a sub set of the enterprise risk management process, a formal IT risk management function should be implemented, with the CIO being accountable for effective IT risk management and a specific person being responsible for ensuring compliance with the required IT risk management practices. Under this process a formal IT risk register should be implemented.
- An IT internal control framework should be implemented, to match the IT risk register. The controls should be designed to clearly specify what actions are to be undertaken, at what frequency, by whom, and what evidence of executing these actions should be retained.
- A formal IT strategic planning process should be implemented, including a procedure for the continual re-alignment of the IT objectives to those of the organisation.
- The impact of IT impact on society and the environment should be considered and how IT could promote sustainability.
- An IT governance framework should be established for the organisation, providing guidance on the process, structures and practices to be implemented to achieve effective IT governance.

- An IT Steering Committee should be established to oversee IT investment, priorities and resource allocation, on behalf of the Board.
- The CIO should be the single point of accountability for IT to the Steering Committee.
- *The IT Steering Committee should also be responsible for overseeing IT strategy and IT investment, priorities and resource allocation.*
- The IT Steering Committee should monitor significant investments for value in terms of IT strategy and appropriateness of resource allocation to the investment. Compliance with the procurement policy should also be monitored.
- An IT vendor management process should be implemented.
- At a minimum, a basic IT value management process should be implemented. Where feasible, IT portfolio management should be implemented to track the value derived from IT investments.
- *IT should implement a reporting framework that provides for:*
  - *Regular operational IT reporting in support of IT line management, at least monthly.*
  - *A quarterly submission to the IT Steering Committee that provides metrics demonstrating IT's contribution to the achievement of key business objectives, as well as areas where the residual risk of critical IT risks is high.*
  - *A summarised version of the IT Steering Committee's report should be submitted to the Board to inform them on IT strategic alignment, value delivery and risk management.*
- A risk assessment process should be implemented that requires at least an annual, comprehensive IT risk assessment and regular (at least six monthly) updates to the IT risk understanding, all of which are documented and monitored in a formal IT risk register.
- The agendas of all risk and audit committee meetings should provide for a section on IT-related risk and control reporting.
- Business continuity management should not be regarded as an IT responsibility, but IT should be able to clearly demonstrate how its IT service continuity planning satisfies business continuity management requirements, as is expected of all departments in the organisation.
- Formal information management practices should be implemented to identify, categorise and classify information. Such practices whould also include monitoring the quality of data and information, compliance with privacy regulations and stakeholderrequirements, and information security management.
- An IT compliance framework should be implemented to ensure that all IT stakeholders', legislative, regulatory and corporate requirements are met.

### 8.4.9 ISO/IEC38500 – Recommendation 14

ISO/IEC38500 provides organisations with six principles for the effective, efficient and acceptable use of IT in their organisations. It is the first formal ISO standard on IT governance. The standard sets out six principles for "good corporate governance of IT", which deal with allocation of responsibility, IT strategy, making acquisitions with business value in mind, IT performance to the agreed service levels, conformance with legislation and regulations, and respect for human behaviour or "the people in the process".

The standard follows and globalises the related, pioneering Australian standard AS-8015 Corporate Governance of Information and Communications Technology and is likely be accepted and implemented globally. At this stage the standard is still limited to a set of principles and does not include detailed guidance on their implementation. South African organisations have been slow in their adoption of ISO/IEC38500. COBIT 5 has incorporated the ISO/IEC38500 direct, evaluate and monitor processes into its own IT governance processes.

#### 8.4.9.1 Implementation Guidance

Participant input indicated that there is no significant appetite for implementing ISO/IEC38500, though it is classified as a "considered" practice. Thus, the following recommendations have been included for organisations which do decide to implement the standard:

- An IT role player matrix should be implemented, showing all roles' responsibilities and accountabilities, as well as which roles need to be consulted or informed in the performance of IT duties.
- Performance management should be implemented at staff, structure and process levels, to monitor how responsibilities are being fulfilled.
- An IT PMO should be implemented if no enterprise PMO exists to manage all projects, including those in IT. The PMO accepts responsibility for the implementation of IT projects.
- The systems development lifecycle and project management methodology should be formalised, as mechanisms for implementing strategy.
- A process should be implemented for integrating IT strategic planning and the operation of the IT PMO, in order to translate IT strategy into execution.
- An IT architecture should be implemented to support the business, application and information architecture layers.
- IT infrastructure management should be implemented, with renewal plans to ensure that the execution of IT strategy is sustained at an infrastructural level.
- Strategic sourcing should be practiced as part of the IT vendor management process.
- An IT assets lifecycle management process should be implemented to support IT planning and ensure the optimal use of IT assets. This should include formal software asset management.
- Formal IT service support and service delivery processes should be implemented to ensure consistent, efficient IT services.
- The key IT metrics should be defined, monitored and reported on, on an ongoing basis.

- Formal processes should be implemented for IT planning, IT service management, project management, the systems development lifecycle, information security management, IT risk management, and enterprise architecture.
- Risk and control self assessment should be implemented as a mechanism to continually monitor compliance.
- IT roles and responsibilities should be formalised, including the following:
  - Formal job descriptions should be implemented;
  - *Where multiple roles are assigned to the same person, care should be taken to ensure that incompatible duties are segregated. Where this is not possible, monitoring and oversight mechanisms and roles should be implemented;*
  - Performance management should be practiced in line with job descriptions;
  - Formal planning should be done for skills development and retention;
  - Formal performance management should be implemented; and
  - *IT people processes should provide for talent management, succession planning and performance management.*

### 8.4.10 IT Sub Processes – Recommendation 15

The IT governance major processes provide the five broad process classes, which require IT sub processes to implement each class. For an effective internal control environment that supports corporate governance, information technology controls need to mature to a level where they could be relied upon to preserve the confidentiality, integrity and availability of information assets. As a prerequisite to an effective system of internal IT control, however, it is necessary to raise IT sub process maturity to a level where controls could be embedded firmly in the process. Low process maturity complicates control over processes and could increase the cost of implementing controls.

Risk assessments drive control design, which is captured in an IT control framework. This is then translated into policies, procedures, standards, and methodologies to implement the required governance mechanisms. Enabling components are broken down into policies, procedures, standards, methodologies, and risk assessments. COBIT 4.1 incorporates process maturity classifications and metrics into the COBIT framework for their use during process formalisation and improvement initiatives. It represents a desirable practice for IT control objectives and a common point of reference for IT professionals and auditors alike. Adopting a COBIT view of the IT environment, 34 processes are distinguishable, which COBIT maps back to the five IT governance major processes, linking the “what” and “how” dimensions of the cube in Diagram 1.

#### *8.4.10.1 Implementation Guidance*

- IT processes should be formalised under each of the IT governance major processes in line with the desirable practices recommended in this paper. Such formalisation should preferably take place in line with the COBIT5 Process Capability Model.
- Each process should be supported by policies, procedures and standards setting out the mechanisms, structures and controls for effective operation of the process.

### 8.4.11 IT Control Framework – Recommendation 16

The IT internal control component represents a significant part of IT governance. It maps the IT internal control environment to the IT risk register, indicating how risks will be mitigated, transferred or avoided. IT controls provide the integrity layer protecting IT business processes. COBIT is the most widely accepted set of control objectives used as the basis for formulating IT controls, but other sources also provide more specific, specialised control objectives, such as those for information security, published under ISO/IEC27000.

#### *8.4.11.1 Implementation Guidance*

- IT controls should be formalised in an IT control framework, applying leading practices, as mentioned above.
- *Prior to adoption of practices, they should be assessed to determine which aspects should be built into the internal control framework.*

### 8.4.12 Supporting Documents – Recommendation 17

The documents "legislating" IT governance in the organisation include policies, standards, procedures and, risk assessments. IT policies lay down the principles that influence and guide the execution of IT procedures and the application of IT standards in line with the philosophy, objectives and strategic plans established by the Office of the CIO. They also describe the consequences of non compliance with the principles they define. Good policies clearly assign roles and responsibilities, explain the rules that should be enforced, with their enforcement mechanisms, and clarify desirable vs. non-desirable behaviour.

Being the owner of these documents, the CIO is accountable for the maintenance and overall enforcement of all IT policies and standards across the organisation. Standards and procedures explain the detail for implementing policies, which are more high-level by nature. The mandatory requirements of individual policies are set out in standards, which describe the desirable outcome of processes and sometimes the minimum configuration requirements for specific technologies, or the minimum performance requirements for specific actions, in support of policies and procedures. Procedures describe the detailed actions to successfully complete a task, that is the process flows for executing IT processes. These procedures belong to the heads of the various IT departments, who are also responsible for the customisation, implementation and maintenance of IT procedures for their individual departments. Risk assessments involve management identifying and analysing relevant risks that could prevent IT from achieving its objectives, as a basis for the design of controls making up the IT control framework.

#### *8.4.12.1 Implementation Guidance*

- *An IT governance framework should be approved by the Board and implemented by the CIO, with oversight by the IT Steering Committee (refer recommendation 13.8).*
- *An IT policy framework should be established specifying what policies, procedures and standards are required to govern each key aspect of IT. The policy framework could be embedded in the IT governance framework or stand separate from it.*
- *IT policies, procedures and standards should be established in line with the IT policy framework. These documents should be reviewed at least annually, with any policy changes being approved by the Board or at least the EXCO. Standard changes may be approved at IT Steering Committee level.*
- *An IT risk register should be established as a sub set of the corporate risk register to detail key IT risks, their level of mitigation and residual risk.*
- *The responsibility for the effectiveness of IT procedures and standards, and for the execution of IT risk assessments, resides with the CIO. Accountability for the effectiveness of IT policies resides with the Board.*
- *An IT charter should be implemented.*

### 8.4.13 Architecture – Recommendation 18

Enterprise architecture is an important mechanism for integrating IT and the business. The enterprise architecture consists of four parts, namely the business, information, application, and technical architecture layers. It is an area that is still in an early stage of maturity at most South African companies, which might make a decision on the adoption of enterprise architecture frameworks prematurely. However, organisations need to start exploring this area and the available tools.

#### *8.4.13.1 Implementation Guidance*

- *IT should actively participate in architectural development, taking ownership of the technology architecture, while aligning to all of the architecture layers.*
- *The CIO should take accountability for the IT architecture.*
- *Business should ideally own the business, application and information architectures, with IT contributing to the latter two layers.*
- *The security architecture laid down by the information security management system (ISMS) should be considered throughout every stage of formulating and maintaining the architecture.*

### 8.4.14 Portfolio Management – Recommendation 19

Portfolio management concerns itself with executing the strategic direction set for investments, including evaluating, prioritising and balancing programmes and services ISACA[a] (2012). It further manages demand within resourcing and financial constraints, based on alignment with strategic objectives, enterprise value and risk. Portfolio management optimises portfolios by including and excluding projects and programmes as priorities change, and monitors portfolio performance on a continual basis. Portfolio management is a developing area which authors view in a number of different ways. The ValIT Framework (IT Governance Institute, 2008), first published by the IT Governance Institute during 2006, provided a useful structure for value delivery and covered portfolio management as one of its three focal areas. ValIT has since been incorporated into COBIT 5. As part of its extension, ITIL 2011 has added the Service Portfolio Management process, which aligns IT services to business.

#### *8.4.14.1 Implementation Guidance*

- Explore how portfolio management will be utilised in future IT investments and management.
- *Where corporate portfolio management is sufficiently mature, IT portfolio management should be practised as a sub set of the corporate process.*
- *Establish a mechanism to align IT spend (and related projects) to organisational objectives and facilitate benefits tracking.*
- *Adopt IT portfolio management, including service portfolio management. If enterprise portfolio management is practised, IT portfolio management should align to the the enterprise process.*
- *Consider how the COBIT5 value management processes could benefit the organisation.*

### 8.4.15 Desirable Practices Conclusion Recommendation 20

In conclusion to this section, it is important to realise that all of the recommended practices are comprehensive and need to be tailored for the organisations implementing them. Setting short to medium term priorities for each adopted practice is key to their successful implementation. Clarity on the aspects adopted from each practice and their priority play and important role in project planning and the accompanying change management to embed such practices.

#### *8.4.15.1 Implementation Guidance*

*To summarise the recommendations in this section, Table 8.1 maps the practices discussed in this paper to the IT governance major processes they are recommended to support. For clarity, RiskIT and ValIT are listed separately, even though they have now been included in COBIT5.*

|  | COBIT | ITIL | PMBOK, Prince2 | ISO/IEC27000 | TOGAF | Balanced Scorecard | Portfolio Management | King III | ISO/IEC38500 | RiskIT | ValIT | ISO/IEC20000 | ISO9001 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Strategic alignment | X | X |  |  | X |  | X | X | X |  |  |  | X |
| Value delivery | X | X | X |  |  |  | X | X | X |  | X |  | X |
| Risk management | X | X | X | X |  |  | X | X | X | X |  |  | X |
| Resource management | X | X | X |  |  |  |  | X | X |  |  | X | X |
| Performance measurement | X |  |  |  |  | X |  | X | X |  |  |  | X |

**Table 8.1 – Practices per IT Governance Major Process**

## 8.5 IT Governance Structure Overview

The proposed roles and structures to implement a generic IT governance framework are described below.

### 8.5.1 Office of the CIO – Recommendation 21

Over the past two decades the role of the CIO has largely focused on deploying IT and controlling costs, however, the CIO's role should be one that is business-oriented, rather than a technically oriented role in order to act as a bridge between IT and the rest of the organisation. Modern CIOs are not only expected to have extensive IT experience but also understand business and the industry it operates in. This section considers four roles traditionally associated with the Office of the CIO, namely the information security officer, technology architect, IT financial manager, and IT risk officer. These are not necessarily full-time positions but areas of responsibilities that are assigned by the Office of the CIO.

New roles being defined for the Office of the CIO include the following:

- IT planning manager – responsible for the creation and maintenance of IT planning, communication of business needs to IT, and education of stakeholders in business on what the IT organisation can do for the business;

- IT programme management office manager – responsible for the effective delivery of the portfolio of IT projects and, by implication for IT project governance, maintaining project management standards, and project monitoring and reporting; and
- IT vendor manager – responsible for managing IT suppliers and the relationship with them, collaborating with business and IT to set sourcing strategies and define vendor oversight processes. This roles requires a procurement expert, who is responsible for monitoring IT vendor viability, especially as far as security and disaster recovery are concerned.

As these three roles have not yet matured and become general practice in IT organisations, they are not included as generic roles in a generic IT governance framework.

#### *8.5.1.1 Implementation Guidance*

- This paper does not insist on the existence of a CTO role. Rather, it is recommended that either the definition of the CIO role be broadened to incorporate the role of the CTO or the roles of the CTO and CIO be clearly segregated.
- The CIO role continues to change and needs to be adjusted continually to keep up with new demands.
- Each organisation should define the CIO role to meet its strategic requirements of IT. These requirements determine the value IT should deliver and consequently the role of the individual leading the function.
- *The Office of the CIO should clearly allocate roles for relationship and demand management.*
- *Application and information ownership remains with business, although IT manages these assets.*

### 8.5.2 Chief Technology Officer – Recommendation 22

The CTO considers the appropriateness of technology acquisitions in view of the IT and organisational strategies, focusing on effectiveness (doing the right things) and efficiency (doing things right). In an organisation where the CTO assumes a technical, engineering role, this role might reside outside the IT department. The CTO role is justified on an organisation-by-organisation basis, depending on the needs and culture of the organisation. It is not a standard role to be found in all IT environments. Some organisations combine the CIO and CTO roles, although in a highly technical engineering or telecommunications environment that might not be possible.

#### *8.5.2.1 Implementation Guidance*

- The creation of a CTO role should be based on a strategic decision and the nature of the organisation. Not all participants in this research would be able to justify a CTO role.
- *Over time, the CTO role is expected to become more prominent, as the CIO role is gradually integrated with business.*

### 8.5.3 Information Security Officer – Recommendation 23

The information security officer (ISO) is responsible for formulating information security policies, procedures and standards aligned to international standards and practice, for example ISO/IEC27000, and for monitoring compliance with approved security policies, procedures and standards. Although no de facto standard for the role of ISO exists, ISACA identifies five job practice areas for ISOs, namely: information security governance, risk management, information security programme development, information security programme management, and incident management and response.

Information security management represents a key area of IT governance, to the extent that some people even wrongly believe it to be the only important area on this topic. It requires a significant level of skill and expertise, which is often not found in other roles. Much debate has taken place as to the most appropriate positioning of the ISO role, with the popular view being that it should exist outside of IT in order to promote its objectivity. However, in most South African organisations, this role continues to function from within IT.

#### *8.5.3.1 Implementation Guidance*

- The ISO role should be clearly defined and segregated from the implementation and administration of these policies, procedures and standards, as the most senior information security oversight function.
- If organisational maturity and culture allow, the ISO role should be based outside IT. At a minimum, information security policy and oversight responsibilities should be segregated from information security administration.

### 8.5.4 Technology Architect – Recommendation 24

The enterprise architecture represents the organising logic for business process and IT infrastructure, reflecting the integration and standardisation requirements of the company's operating model. It provides a long-term view of a company's processes, systems and technologies so that individual projects can build capabilities.

The chief enterprise architect segregates the enterprise architecture layers and outlines the architecture of each layer, formulates architectural standards and monitors compliance with these standards. An Enterprise Architecture Forum typically oversees the definition of architectural standards, alignment of the IT organisation with organisational objectives and the maintenance of architectural integrity, as well as instituting action against parties that do not comply with architectural standards.

The technology architect liaises with the chief enterprise architect and other architects to facilitate the development of the IT architecture and its alignment to the business, application and information architectures. Many South African companies still incorrectly regard enterprise architecture as an IT responsibility, so most achitecture functions start off from within IT. Enterprise architecture is still a relatively young, evolving function, with organisations coming to terms with architecture principles and practice.

#### 8.5.4.1 Implementation guidance

- *Regardless of the positioning of enterprise architecture and the manner in which it is resourced, a key principle that should be adhered to is that the enterprise architecture, inclusive of the IT architecture role, should not be outsourced.*
- *The IT architecture role should be formalised to fulfil IT's responsibility to the organisational architecture function.*
- *Enterprise architecture should not be an IT responsibility. Application and information architecture should preferably not be either.*

### 8.5.5 IT Financial Manager – Recommendation 25

The IT financial manager role could justify a full-time position in many large IT organisations, but it could also be a support function provided by the finance department. It involves the following responsibilities:

- Overseeing the capital and operational IT budgeting process and monitoring actual vs. budgeted IT expenditure;
- Depending on the maturity of the organisation, costing of IT services per the service catalogue to the various end-user departments, and, if required by policy, charging these costs back to the individual departments;
- Monitoring compliance of IT procurement with organisational policies and procedures, and with IT hardware, software and service standards; and
- Monitoring IT programme spend at the portfolio level.

#### 8.5.5.1 Implementation Guidance

The IT financial management role should be formally assigned in all environments, but the feasibility of creating a full-time position around it should be carefully evaluated based on the size and complexity of the environment. *Where feasible, this should be a full-time role.*

### 8.5.6 IT Risk Officer – Recommendation 26

Many publications exist on ERM and its direct sub processes, yet few comprehensive works have been published on the IT Risk Management specialisation. RiskIT defined the IT risk management process model in three domains, namely: Risk Governance, Risk Evaluation and Risk Response. It assigned accountability for IT risk management to the chief risk officer, but made provision for the creation of an IT risk officer role. COBIT 5 incorporates RiskIT, which adds much more emphasis on IT risk management. The IT risk officer role could be a sub set of the IT governance officer role or a sub role within the ERM function.

#### *8.5.6.1 Implementation Guidance*

- A formal IT risk officer role should be created, either as a full-time position or as a role compatible with another IT governance or enterprise risk management role. The IT risk officer role could also be combined with an IT governance officer role. *Where feasible, this should preferrably be a full-time role.*
- *IT risk management should remain a key responsibility of all IT managers and a responsibility of all line managers relying on IT services to enable their areas of responsibility.*
- *If the organisation has a combined assurance forum, the IT risk officer should actively participate in the forum.*
- *The IT risk officer is responsible for overseeing the record and tracking of all high-risk entries in the IT risk register, as well as monitoring IT control deficiencies resulting in areas of high residual risk.*

### 8.5.7 Applications Manager – Recommendation 27

The applications manager is responsible for managing applications through their lifecycle. He or she could play a significant role in systems development, although that is not a prerequisite. The applications manager is the custodian of technical application management knowledge and expertise and provides the balance between the cost and skills level of application management staff. He or she also provides the resources to support the IT service management lifecycle and integrates the Application Management Lifecycle into the IT Service Management Lifecycle. The applications manager guides IT operations on ongoing operational management of applications. Taking a broad view on the role of the applications manager, he or she is also responsible for:

- Monitoring the performance and operation of applications, whether batch or on line, in real time;
- Application data integrity;
- Application performance tuning;
- Application patch management; and
- Monitoring application integrity, more specifically ensuring that the change and release and deployment procedures are complied with as far as applications are concerned.

#### *8.5.7.1 Implementation Guidance*

- *The leadership roles for development and support should be segregated to provide for development management and applications management respectively.*
- *The development, testing and support environments should be segregated. Roles for each of these environments should be segregated accordingly.*

### 8.5.8 Technical Manager – Recommendation 28

The technical manager is the custodian of technical knowledge and expertise related to managing the IT infrastructure. This role resources the technical infrastructure supporting the IT service management lifecycle, from service design through service operation and continual technology improvement. The technical manager is also responsible for guiding the operations manager on ongoing operational management of technology. It cannot be dictated whether the technical manager or the application manager owns and is responsible for the IT service support and IT service delivery processes.

#### *8.5.8.1 Implementation Guidance*

The technical management role should be clearly defined and assigned to an individual who will be responsible for all aspects of technical management, including infrastructural projects and technical architecture.

### 8.5.9 Operations Manager – Recommendation 29

In a large IT environment, the number of operations staff and sometimes the number of facilities warrant the appointment of an operations manager. This usually depends on the size of the department. The operations manager is responsible for:

- Operations control, including console management, job scheduling, backup and restoration, print and output management, recording and monitoring operational logs, and maintenance activities on behalf of application and technical management;
- Maintaining shift and operations schedules, managing and resourcing operational shifts, and maintaining reports on operational activities;
- Managing the physical environment (facilities), including data centres and recovery facilities, and, where required, managing consolidation of facilities;
- Maintaining and managing standard operating procedures, and ensuring compliance with operational service and infrastructural standards to maintain a stable operating environment; and
- Responding to business needs for scaling infrastructural capacity to levels that effectively supports continually changing or expanding IT services.

#### *8.5.9.1 Implementation Guidance*

- *Each organisation should evaluate whether or not the size of its IT department justifies the appointment of separate operations and technical manager roles. If not, the technical manager role could be combined with that of the operations manager.*
- *A dedicated IT service support manager should be appointed, distinct from the technical manager and operations manager roles.*
- *The IT service delivery manager role could be a dedicated responsibility or could be assigned to the IT operations manager.*
- *This research does not argue for any particular IT operations structure, but recommends (i) clear roles and responsibilities for each operational area, and (ii) a clear definition of the operations management role.*

### 8.5.10 IT Strategy Committee – Recommendation 30

Traditional thinking used to dictate that the IT Strategy Committee be composed of Board members and non-Board executives, including the CIO. It assisted the Board in governing and overseeing the enterprise's IT-related matters and had to ensure that IT governance was addressed formally, as well as that the Board had the information required to ensure effective governance over IT.

The IT Strategy Committee concerns itself with the alignment of IT to organisational objectives, more specifically, how IT delivers against strategy, how IT investments support the current and future needs of the organisation, and focusing IT on specific organisational objectives that are dependent on IT enablement. This research found that the participating organisations no longer segregated the IT Strategy and IT Steering Committees, which appears to have become common practice.

#### *8.5.10.1Implementation Guidance*

*Organisations should combine the IT Strategy Committee and IT Steering Committee by creating a specific sub agenda covering IT strategy oversight.*

### 8.5.11 IT Steering Committee – Recommendation 31

The IT Steering Committee is at the executive level and focuses on tracking IT investment, setting priorities for IT and allocating scarce IT resources. It typically combines senior business executives and IT management, with its membership often being indicative of the view of IT value in the organisation. Contextualising the 2003 view of the IT Governance Institute with developments since, its role could be equated to that of an IT portfolio management committee, as most of the responsibilities assigned to it by the IT Governance Institute maps onto the IT portfolio management process. The Committee meets regularly to provide direction and oversight for IT across the enterprise. The IT Steering Committee is closely associated with IT service and project governance, and provides guidance and oversight for all other IT Steering Committees. Furthermore, it governs strategic functions including architecture, planning and vendor management.

#### *8.5.11.1 Implementation Guidance*

- Organisations should have an IT governance body responsible for overseeing the establishment of mechanisms for delivering the strategy, typically in the form of an IT Steering Committee.
- *Unless a separate IT Strategy Committee has been established, the IT Steering Committee should oversee IT strategy formulation.*
- *The IT Steering Committee membership should include an adequate representation by executive committee members, from whom the chair should also be selected.*
- *The IT Steering Committee should provide oversight only and not partake in any decision making, which remains a line management responsibility.*

### 8.5.12 Technology Architecture Forum – Recommendation 32

Top management, with the IT leadership, has the responsibility of establishing general enterprise architecture principles, while the Technology Architecture Forum oversees the establishment of and compliance to tecnology architecture standards, as well as the alignment of the IT architecture to other architecture layers. As part of the extended IT organisation the Enterprise Architecture Forum oversees the structure of the extended IT organisation and how it relates to the organisation overall.

#### *8.5.12.1 Implementation Guidance*

- It is recommended that a governance body, for example a Technology Architecture Forum, be established to oversee the establishment and effectiveness of the technology architecture in the organisation.
- *This forum should report to the CIO and concern itself with the establishment of technology standards, as well as the oversight over the technology architecture and its supporting standards.*
- *Ideally, enterprise architecture should report into corporate strategy.*

### 8.5.13 Programme Management Office – Recommendation 33

The IT PMO oversees the execution of programmes and projects in fulfilment of the strategic objectives of IT, as a sub set of the wider portfolio of projects in the organisation. The PMO also develops and enforces programme and project standards, reports on progress and assists in obtaining approval of project budgets. The IT PMO reports to the EPMO, whose influence extends beyond one business unit or functional area. In some organisations, IT programmes and projects are driven by the EPMO, while others create an IT PMO for that purpose. As long as both apply strong programme and project management principles and follow consistent methodologies, there is little difference between the two approaches. At the enterprise level, the portfolio management process aligns programmes (collections of projects with shared objectives) to organisational objectives. Diagrammatically, this could be depicted by three concentric circles, with the innermost circle representing projects, the middle circle programmes and the outer circle portfolios of programmes.

#### *8.5.13.1Implementation Guidance*

- PMO principles should be adopted to govern any significant IT projects.
- A formal, standardised project management methodology should be implemented, including a project management maturity model, with maturity targets, whether for IT or at an enterprise level.
- *The decision to implement a centralised or decentralised PMO should reflect the culture of the organisation.*
- *Where an EPMO exists, IT should preferably be an instance thereof.*

### 8.5.14 IT Governance Roles – Recommendation 34

To summarise the recommendations on IT management roles in this section, *Table 8.2* maps the roles discussed in this paper to the IT governance major processes they are recommended to support.

| | CIO | CTO | ISO | Applications Manager | Technology Architect | Technical Manager | Operations Manager | IT Financial Manager | IT Risk Officer |
|---|---|---|---|---|---|---|---|---|---|
| Strategic alignment | R | R | I | C | R | C | I | C | R |
| Value delivery | R | C | C | R | C | R | R | R | C |
| Risk management | R | R | R | R | R | R | R | R | R |
| Resource management | R | R | C | R | I | R | R | R | C |
| Performance measurement | R | R | R | R | C | R | R | R | R |

**Table 8.2 – IT Management Roles per IT Governance Major Process**

### 8.5.15 IT Governance Structures – Recommendation 35

To summarise the recommendations on structures in this section, *Table 8.3* maps the structures discussed in this paper to the IT governance major processes they are recommended to support.

|  | Board | Office of the CIO | IT Steering Committee | IT Strategy Committee | Technology Architecture Forum |
|---|---|---|---|---|---|
| Strategic alignment | A | R | C | A | R |
| Value delivery | A | R | A | C | C |
| Risk management | A | A | I | I | C |
| Resource management | I | A | C | I | C |
| Performance measurement | I | A | I | I | C |

**Table 8.3 – RACI Mapping for IT Governance Structures**

## 8.6 Recommended Approach to Implementing the Final, Amended PES IT Governance Framework

The framework is intended to be comprehensive and sufficiently generic to address all key aspects of governance a large organisation might require, yet be a non-prescriptive tool that is open to interpretation and customisable to suit the requirements of the organisation implementing it. All recommendations are discretionary, although organisations should be able to address the highlighted areas if an effective IT governance framework is to be implemented. Like any other significant initiatives, implementing the framework should be subjected to formal project management principles, with a formal change management work stream, under oversight of the IT Steering Committee.

## 8.7 Other Considerations

One of the questions raised during the research was how the framework applies to cloud computing. At this stage, organisations are still formulating their positions on cloud, so the recommendation is that this topic should be dealt with through a combination of strategy, architecture, service level management, risk management, and vendor management. Cloud computing has not been included explicitly in this research.

## 8.8 Conclusion

The final, amended PES Framework provides a single, cohesive view of all aspects of IT governance that are appropriate for most large organisations. The framework supports the implementation of customised processes, enablers and structures required for effective IT governance in the various organisations involved in this research.  Such an implementation could be tailored to focus on specific compliance objectives under, for example, a King III or ISO/IEC38500 project.

# Chapter Nine: Conclusion

## 9.1 Introduction

The premise of this research was that there are arguments towards the fact that no universal framework exists that is appropriate for most large organisations; no single, cohesive view of IT governance exists in most organisations; and there is an inadequate understanding of the concept of an IT governance framework in most global organisations. Based on this, it appeared as if there was no single, generic IT governance framework that would enable organisations to formulate their own IT governance frameworks. Despite COBIT 5 being positioned as an all-encompassing IT governance framework, it has not been proven as such, and South African organisations are still working on establishing an effective way of dealing with their IT governance needs.

Regulatory pressures are at an all-time high and continue to become ever more stringent in the process necessitating IT governance structures customised to organisational needs and enabling rather than disabling successful business practices. Compliance fatigue sometimes relegates IT governance programmes to a "tick-the-box" exercise, which is why the PES IT Governance Framework is a timeous tool to facilitate a "just enough" governance solution.

## 9.2 Contributions of the Research

The PES Framework provides a single, cohesive view of all aspects of IT governance that are appropriate for most large organisations, thus addressing the need for a generally relevant IT governance framework. By agreeing to a commonly acceptable IT governance framework, the participants have moved closer to a single view on what constitutes effective IT governance and what an IT governance framework should look like.

The PES IT Governance Framework supports the implementation of customised processes, enablers and structures required for effective IT governance in the various organisations involved in this research. Such an implementation could be tailored to focus on specific compliance objectives under, for example, a King III or ISO/IEC38500 project. The input which the various CIOs provided has contributed to the outcome of this research being more representative of the needs of the South African IT community, and reflecting practical recommendations for implementing IT governance processes, enablers and structures.

The final, amended PES IT Governance Framework incorporates the elements required to implement an IT governance framework, as required by King III. Through a set of practical recommendations it utilises popular standards and practices like COBIT 5, ITIL, Prince2 and ISO/IEC27001 to enable the implementation of an IT governance framework. The organisations participating in the research confirmed what processes, enablers and structures are feasible for them, in order to refine the theoretical PES IT Governance Framework into a product they would all be able to implement.

The research sucessfully confirmed the feasibility of the proposed PES IT Governance Framework, incorporating participant input and producing a generic IT governance framework that could be applied to any large organisation in South Africa.

One aspect that did not receive the anticipated support and was therefore not addressed as comprehensively as expected, was the concept of green IT, which supports IT sustainability. The research participants consider enabling business to be a going concern as much more important to IT sustainability than green IT.

## 9.3 Limitations of the Study

One aspect that could have been incorporated into the IT governance framework, is sustainability, as required by King III.

## 9.4 Recommendations for Future Research

The research and related interaction with industry highlighted the following areas for future research:

### 9.4.1 COBIT 5

A deluge of COBIT 5 publications have been produced, however, a low adoption rate bears testimony to the difficulty organisations have in understanding the material and finding practical application for it, amid stark economic realities. The alignment of IT governance frameworks built during the early days of King III to COBIT 5 would be of value.

### 9.4.2 IT Value Management

A commonly accepted view and supporting definitions of what constitutes IT value, together with the tracking and reporting of IT value realisation, should be explored.

### 9.4.3 IT Reporting Framework

A common IT reporting framework should be developed that presents appropriate levels of detail to the Board for King III purposes, to the Executive and IT Steering Committee for oversight purposes, and to IT management for operational purposes.

## 9.5 In Closing

The interaction with CIOs from leading South African organisations has confirmed the absence of a commonly accepted IT governance framework but highlighted the areas of priority for IT governance to be incoporated into the PES IT Governance Framework.

The PES IT Governance Framework, paying attention as it does to an improved concept of an IT governance framework comprising a single, cohesive view that is universal and contemporary, goes a long way to resolving large corporates' IT governance concerns. Large corporates could benefit greatly from considering this PES IT Governance Framework for adoption.

# Bibliography

ADDY, R. (2007) Effective IT Service Management – To ITIL and Beyond! Springer-Verlag Berlin Heidelberg. 2007

AL-ZWYALIF, I. (2013) IT Governance and its Impact on the Usefulness of Accounting Information Reported in Financial Statements. International Journal Of Business & Social Science [serial online]. February 2013;4(2):83-94. Available from: Business Source Complete, Ipswich, MA. Accessed August 8, 2013

ALI, S. (2006) Effective information technology governance mechanisms: An Australian Study. Gadjah Mada International Journal of Business. January- April 2006. Vol. 8, No. 1

ALI, S., GREEN, P., ROBB, A. (2013) Measuring Top Management's IT Governance Knowledge Absorptive Capacity. Journal Of Information Systems [serial online]. Spring2013 2013;27(1):150. Available from: Business Source Complete, Ipswich, MA. Accessed July 31, 2013

ASHFORD, W. (2008) Cranfield and Deloitte sound death knell for CIOs. Computer Weekly. 9-12-2008:7

ATOS CONSULTING, 2007 IT governance in the extended enterprise. ATOS Consulting, Utrecht, The Netherlands. 2007

BAMBERGER, J. AND ULSCH, M. (2006) Sound IT governance requires breadth and depth. Financial Executive, March 2006:56

BARBER, K. ED. (2004) The Canadian Oxford Dictionary. Oxford Reference Online. Oxford University Press. Rhodes University Library. 22 February 2009

BASCHAB, J., PIOT, J. (2007) The executive's guide to information technology. John Wiley & Sons. 2007:322

BETZ, C.T. (2007) Architecture and patterns for IT service management, resource planning, and governance: making shoes for the cobbler's children. Charles T. Betz. Publisher Amsterdam; Boston, MA: Elsevier Morgan Kaufmann. 2007

BIN SAHIBUDDIN, S., NABIOLLAHI, A. (2008) Considering Service Strategy in ITIL V3 as a Framework for IT Governance. IEEE (978-1-4244-2328-6/08). 2008

BLOCH, M., HOYOZ-GOMEZ, A., 2009 How CIOs should think about business value, McKinsey & Company, McKinsey on Business Technology, Spring 2009

BLOEM, J (2006) Making IT governance work in a Sarbanes-Oxley world. Wiley, 2006:251

BOONEN, H., BRAND, K. (2007) IT Governance based on COBIT 4.0. Van Haren Publishing. 2007

BORCK, J.R. (2001) A Balancing Act to ROI. Infoworld. 23 July 2001

BOTTGER, P. (2008) Leading in the top team: the CXO challenge / edited by Preston Bottger. Publisher Cambridge, UK; New York: Cambridge University Press. 2008

BOULTON, R.W., LIANG, .H., XUE, Y. (2008) Information technology governance in information technology investment decision processes: the impact of investment characteristics, external environment, and internal context. MIS Quarterly Vol. 32 No. 1: 68. 2008

BRESLIN, G. (2011) Collins English Dictionary. HarperCollins Publishers. Eleventh Edition. 2011

BROADBENT, M. AND KITZIS, E.S. (2005) The New CIO Leader – Setting the Agenda and Delivering Results. Marianne Broadbent, Ellen S. Kitzis. Gartner, Inc. Harvard Business School Press. Boston, Massachusetts. 2005

BROWN, A.E., GRANT, G.G. (2005) Framing the Frameworks: A Review of IT Governance Research. Communications of the Association for Information Systems. Volume 15, 2005: 696-712

BROWN, VAN METRE, E. (2008) Role Profile: The CIO – Understanding And Marketing To The CIO Professional, Forrester Research, Inc. 18 December 2008

BROWN, J.T. (2008) The Handbook of Program Management. McGraw Hill, Two Penn Plaza, New York, NY. 2008

BRUCE, G. (2005) Six Sigma for Managers. McGraw Hill Companies, Inc. 2005

BUTLER, M.J.., BUTLER, R. (2010) Beyond King III: Assigning accountability for IT governance in South African enterprises. South African Journal of Business Management. Sep2010, Vol. 41 Issue 3, p43

CA (2008) Business Service Management Links IT Services to Business Goals. CA. 2008

CALDER, A. (2006) Implementing Information Security based on ISO 27001/ ISO 17799 – A Management Guide. Van Haren Publishing. 2006

CAMBRIDGE (2015) dictionary.cambridge.org/us/dictionary/business-english [accessed 25 February 2015]

CAPGEMINI (2008) TOGAF 9 Draft 4. September 5, 2008:651

CECERE, M. (2009) Role Descriptions For The Office Of The CIO – Key Roles Support The CIO In Driving IT's Success, Forrester Research, Inc., 22 October 2009

CECERE$^{a}$, M. (2009) Global Initiatives Require Enterprise IT Executive Committees, Forrester Research, Inc., 22 October 2009

CHUI, M., EDIN, P., MANYIKA, J. Time to raise the CIO's game. McKinsey & Company, Number 17, Autumn 2009

CMA MANAGEMENT (2008) IT a crucial piece of the risk management pie. May 2008:10

CNN edition.cnn.com/2010/WORLD/europe/06/08/france.trader.trial/index.html?iref=allsearch

COLLINS (2015) www.mycobuild.com/Results.aspx [accessed 25 February 2015]

CONGER, S., DATTERO, R., GALLUP, S.D., J.J. QUAN (2009) An Overview of IT Service Management. Communications of the ACM. May 2009. Vol. 52. No 5

COSO (2004) Committee of Sponsoring Organisations of the Treadway Commission (COSO) – *Enterprise Risk Management Framework*. USA. September 2004

COSTELLO, T., LAPLANTE, P. (2006) CIO Wisdom II – More Best Practices. Pearson Education, Inc., Upper Saddle River, N.J. 2006

CRAWFORD, J.K. (2007) Project management maturity model. Boca Raton, FL: Auerbach Publications. 2007

DATAMONITOR (2007) www.datamonitor.com. November 2008:189

DATAMONITOR (2008) www.datamonitor.com. December 2008:203

DE HAES, S., VAN GREMBERGEN, W. (2004) IT Governance and Its Mechanisms. Information Systems Control Journal, Volume 1, 2004

DE HAES, S., VAN IT Governance Implementation Guide. In W. van Grembergen, & S. De Haes (Eds.), Implementing Information Technology Governance: Models, GREMBERGEN, W. (2008) Practices and Cases. Hershey, PA. 2008:238

DE HAES, S., VAN GREMBERGEN[a], W. (2008) IT Governance in Practice: Six Case Studies. In W. van Grembergen, & S. De Haes (Eds.), Implementing Information Technology Governance: Models, Practices and Cases. Hershey, PA. 2008:26

DE HAES, S., VAN GREMBERGEN[b], W. (2009) An Exploratory Study into IT Governance Implementations and its Impact on Business/IT Alignment. Information Systems Management. Spring2009, Vol. 26 Issue 2, p135.

DE HAES, S., VAN GREMBERGEN[c], W. (2009) Demonstrating the Value of COBIT and Val IT IT Governance Practices. Information Systems Control Journal, Volume 5, 2009

DEBRECENY, R., GRAY, G. (2013) IT Governance and Process Maturity: A Multinational Field Study. Journal Of Information Systems [serial online]. Spring2013 2013;27(1):182. Available from: Business Source Complete, Ipswich, MA. Accessed July 31, 2013

DEBRECENY, R., DE HAES, S., VAN GREMBERGEN, W. (2013) COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. Journal Of Information Systems [serial online]. Spring2013 2013;27(1):308. Available from: Business Source Complete, Ipswich, MA. Accessed July 31, 2013

DVIR, D., SHENHAR, (2007) Reinventing Project Management: the diamond approach to successful growth and innovation. Harvard Business School Press, Boston, Massachusetts. 2007

EHLERS, M.B., LAZENBY, J.A.A. EDS. (2004) Strategic Management – Southern African Concepts and Cases. Van Schaik Publishers. South Africa. 2004:149

EPSTEIN, M.J., REJC, A. (2005) How to Measure and Improve the Value of IT – a Balanced Scorecard Geared Toward Information Technology Issues Can Help You Start the Process. Strategic Finance. October 2005:41

EVERINGHAM, G. AND WIXLEY, T. (2005) Corporate Governance. Second edition. Siber Ink. 2005:91

EY (2012) The DNA of the CIO. EYGM Limited. 2012:4-7

EY (2013) Business Pulse – Exploring dual perspectives on the top 10 risks and opportunities in 2013 and beyond – Global Report. EYGM Limited. 2013:4-

34

EY$^{a}$ (2013) Performance. Volume 5, Issue 1. EYGM Limited. 2013:P33-34

FICHADIA, A., RAVAL, V. (2007) Risks, controls and security: concepts and applications. Hoboken, N.J. Wiley. Chichester: John Wiley. 2007

FILIPEK, R. (2008) Security tops technology trends. Internal Auditor. The Institute of Internal Auditors. February 2008

FORRESTER RESEARCH, INC. (2007) Defining IT GRC. December 4, 2007

FRESCHI, C. (2009) A maturing industry faces the need for standards. SECURITV. January 2009:48

GERRARD, M., SHORT, J. (2009) IT Governance Must Be Driven by Corporate Governance, Gartner, Inc., 17 November 2009

GARTNER, INC. (2008) The ‘Seven Deadly Sins’ of Application Governance. Gartner Research. ID Number: G00155896. 26 March 2008

HANDLER, R., MAIZLICH, B. (2005) IT Portfolio Management Step-by-Step – Unlocking the Business Value of Technology. Wiley and Sons, Inc. Hoboken, New Jersey. 2005

HANDLER, R.A. (2009) Role Overview: Chief Enterprise Architect, Gartner, Inc., 17 December 2009

HAMAKER, S (2004) Principles of IT Governance. Information Systems Control Journal. Volume 2, 2004

HAMAKER, S AND HUTTON, S (2005) Enterprise Governance and the Role of IT. Information Systems Control Journal. Volume 6, 2005

HANDLER, R.A. (2009) Role Overview: Chief Enterprise Architect, Gartner, Inc., 17 December 2009

HEWLETT-PACKARD DEVELOPMENT COMPANY. L.P. (2007) The HP Service Management Framework. Hewlett-Packard Development Company, L.P. 2007

HOSKE, M.T. (2009) Standards, more or less. Control Engineering. January 2009:31

INABA.,Y., SHIBUYA, H. (2013) Executive Management Must Establish IT Governance: Tokio Marine Group. COBIT Focus [serial online]. January 2013;2013(1):8-13. Available from: Business Source Complete, Ipswich, MA. Accessed July 31, 2013

ISACA (2008) Defining Information Security Management Position Requirements – Guidance for Executives and Managers. 2008

ISACA (2012) ISACA. COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT. 2012

ISACA$^{a}$ (2012) ISACA. COBIT 5 – Enabling Processes. 2012

ISACA$^{b}$ (2012) ISACA. COBIT 5 – Implementation. 2012

ISO/IEC1779 (2005) International Standard ISO/IEC17799 – Information technology — Security techniques — Code of practice for information security management, second edition. International Standards Organisation. Geneva. Switzerland. 2005-06-15

ISO/IEC27001 (2005) International Standard ISO/IEC27001 – Information Technology – Security Techniques – Information Security Management Systems – Requirements, first edition. Geneva. Switzerland. 2005-10-15

ISO (2008) International Standard ISO/IEC38500 – Corporate governance of information technology. International Standards Organisation. Geneva. Switzerland. 2008-06-01

INSTITUTE OF DIRECTORS SOUTHERN AFRICA (2009) King Report on Governance for South Africa. Institute of Directors Southern Africa. 2009. [Online]. Available at: http://african.ipapercms.dk/IOD/KINGIII/kingiiireport [Accessed 14 March 2010]

IT GOVERNANCE INSTITUTE (2003) Board Briefing on IT Governance, Second Edition. 2003

IT GOVERNANCE INSTITUTE (2004) The IT Governance Institute. Mapping of PMBOK with COBIT 4.0, IT Governance Institute, 2004

IT GOVERNANCE INSTITUTE (2006) COBIT Mapping – Overview of International IT Guidance, 2nd Edition. 2006

IT GOVERNANCE INSTITUTE$^{a}$ (2006) Enterprise Value: Governance of IT Investments – The Val IT Framework. 2006

IT GOVERNANCE IT Control Objectives for Sarbanes-Oxley – The Role of IT in Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition.

INSTITUTE[b] (2006) September 2006

IT GOVERNANCE INSTITUTE (2007) Control Objectives for Information and Related Technology (COBIT) 4.1. 2007

IT GOVERNANCE INSTITUTE (2007) Mapping of Prince2 with COBIT 4.0. 2007

IT GOVERNANCE INSTITUTE (2008) Enterprise Value: Governance of IT Investments – The Val IT Framework 2.0. 2008

IT GOVERNANCE INSTITUTE[a] (2008) IT Governance Global Status Report—2008. IT Govermance Institute. 2008

IT GOVERNANCE INSTITUTE (2009) Enterprise Risk: Identify, Govern and Manage IT Risk – The Risk IT Framework. Exposure Draft v0.1. 3 February 2009

IT GOVERNANCE INSTITUTE[a] (2009) Mapping of ITIL v3 With COBIT® 4.1, IT Governance Institute, 2009

IT GOVERNANCE INSTITUTE (2011) Global Status Report on the Governance of Enterprise IT (GEIT) — 2011, IT Govermance Institute. 2011

JEWER, J., McKAY, K. (2012) Antecedents and Consequences of Board IT Governance: Institutional and Strategic Choice Perspectives. Journal Of The Association For Information Systems [serial online]. July 2012;13(7):582. Available from: Business Source Complete, Ipswich, MA. Accessed July 31, 2013

KAIRAB, S. (2005) A Practical Guide to Security Assessments. Auerbach Publications, CRC Press LLC, 2005

KAPLAN, R.S., NORTON, D.P. (1996) The balanced scorecard: translating strategy into action. Boston, Massachusetts. Harvard Business School Press. 1996

KAPLAN, R.S., NORTON, D.P. (2004) Strategy maps. Harvard Business School Press. Boston, Massachusetts. 2004:13

KAPLAN, R.S., NORTON, D.P. (2006) Translating Strategy into Action – The Balanced Scorecard. Harvard Business School Press. Boston, Massachusetts. 2006

KARK, K., OTHERSEN, M., MCCLEAN, C. Defining IT GRC. Forrester Research, Inc. 2007

(2007)

KENDALL, G.I. (2003) Advanced project portfolio management and the PMO: multiplying ROI at warp speed. Boca Raton, Fla.: J. Ross Pub. ; [S.l.]: International Institute for Learning. 2003

KERZNER, H. (2005) Using the project management maturity model. 2nd edition. 2005

LUFTMAN, J.N. (2004) Managing the Information Technology Resource. Pearson Education, Inc., Upper Saddle River, N.J. 2004

LE VEQUE, V. (2006) Information Security, A Strategic Approach. Wiley-Interscience. Hoboken, NJ: John Wiley & Sons. 2006

LUIPERS, J., VAN STEENBERGEN, M., VAN DEN BERG, M., WAGTER, R. (2005) Dynamic enterprise architecture – how to make it work. Hoboken, NJ: John Wiley & Sons. 2005

M2PRESSWIRE (2009) The Rise of Enterprise Architectures – and the integration of IT into the business Out Now. M2PressWIRE; 06/18/2009

MAHONEY, J. (2008) Summarising the Changing Shape of IT and its Implications, Gartner, Inc., 2008

MARKS,N. (2010) The Pulse of IT Governance. INTERNAL AUDITOR. August 2010, Vol. 67 Issue 4, p34

MCPHIE, D. (2000) AICPA/CICA SysTrust Principles and Criteria. Journal of Information Systems, Vol. 14, Supplement. 2000

MERRIAM-WEBSTER WORD CENTRAL (2015) http://www.wordcentral.com/cgi-bin/student?book=Student&va=framework [accessed 25 February 2015]

MOELLER (2008) Sarbanes-Oxley internal controls: effective auditing with AS5, COBIT and ITIL. Hoboken, NJ: John Wiley & Sons. 2008

MOTLAGH, S.M., SABEGH, A.J. (2012) The role and relevance of IT governance and IT capability in Business – IT alignment in medium and large companies. Business and Management Review Vol. 2(6). August, 2012:21

MYERS, M.D (1997) Qualitative Research in Information Systems. MIS Quarterly. 21, 2: 241-242. MISQ Discovery, archival version, June 1997. [Online]. Available at: http://www.misq.org/discovery/MISQD_isworld/. MISQ Discovery, updated version, last modified: January 4, 2008. Available at:

http://www.qual.auckland.ac.nz. [Accessed 13 February 2008].

NATIONAL COMPUTING CENTRE (2005) IT Governance – Developing a successful governance strategy – A Best Practice guide for decision makers in IT. 2005

NIVEN, P. R. (2006) Balanced Scorecard Step-By-Step: maximizing performance and maintaining results. Hoboken, NJ: John Wiley & Sons. 2006

NOLAN R., McFARLAN, F.W. (2005) Information Technology and the Board of Directors. Harvard Business Review. October 2005. Pp1-8

OFFICE OF GOVERNMENT COMMERCE (2000) Service Support – The IT Infrastructure Library (ITIL). 2000

OFFICE OF GOVERNMENT COMMERCE (2001) Service Delivery – The IT Infrastructure Library (ITIL). 2001

OFFICE OF GOVERNMENT COMMERCE (2007) Service Operation. Office of Government Commerce. The Stationery Office. 2007

OFFICE OF GOVERNMENT COMMERCE (2009) Managing Successful Projects with PRINCE2. 2009

OLVE, N., SJOSTRAND, A. (2006) Balanced Scorecard. Chichester. Capstone Publishing. 2006

OUD, E.J. (2005) The value to IT of using international standards. Information Systems Control Journal. Volume 5, 2005.

PELTIER, T.R. (2004) Information Security Policies and Procedures – A practitioner's reference. Auerbach Publications. 2004

PETERS, A. (2012) Forrester- Five important guidelines for business technology governance. Computer Weekly. 10/30/2012:p15

PETERSON, R. (2004) Crafting Information Technology Governance. www.ism-journal.com, Fall 2004:8

POLLARD, C., RIDLEY, G., WEBB, Attempting to Define IT Governance: Wisdom or Folly? Proceedings of the 39th Hawaii International Conference on System Sciences. 2006

P. (2006)

PROJECT MANAGEMENT INSTITUTE (2004) A Guide to the Project Management Body of Knowledge – Third Edition (PMBOK Guide). Newtown Square. Pennsylvania. USA. 2004

PYZDECK, T. (2003) The Six Sigma Handbook. The McGraw Hill Companies, Inc. 2003

RAGHUPATHI, W. (2007) Corporate governance of IT: A framework for development. Communications of the ACM. Vol 50, No. 8: 95-96. 2007

RAJEGOPAL, S. (2007) Project Portfolio Management: Leading the Corporate Vision. Basingstoke [Enland]. New York: Palgrave Macmillan. 2007

RAU, K.G. (2004) Effective governance of IT: design objectives, roles and relationships. Information systems management. Fall 2004

REINHARD, J. (2013) IT Governance INTEGRATION. Internal Auditor [serial online]. August 2012;69(4):51. Available from: Business Source Complete, Ipswich, MA. Accessed July 31, 2013

RILEY, J. (2005) Computer Weekly. 27-09-2005:10

ROBERTSON, D., ROSS, J.W. AND WEILL, P.(2006) Enterprise architecture as strategy: creating a foundation for business execution. Harvard Business Press. Boston, Massachusetts. 2006

ROMERO, S. (2012) An IT governance confusion solution. INTERNAL AUDITOR. FEBRUARY 2012, Vol. 69 Issue 1, p69. 2012

ROOS, P.C. (2004) IA Adviser. Implementing an IT Governance Framework. July 2004:10-13

ROSS, .J.W., WEILL, P. (2009) IT savvy – what top executives must know to go from pain to gain. Harvard Business Press. Boston, Massachusetts. 2009

SANDRINO-ARNDT, B. (2008) People, Portfolios and Processes: The 3P Model of IT Governance. Information Systems Control Journal, Volume 2, 2008:1

SANDRINO-ARNDT, B., (2009) IT Governance Implementation Using the 3P Model—A Staged Approach. ISACA JOURNAL VOLUME 3, 2009

SARAN, C. (2007) Enterprise architectures must be able to show business value, Gartner says. Computer Weekly; 10/2/2007:18

SCOTT, J. (2008) EA Team Structures Vary Widely. Forrester Research, Inc. April 11, 2008

SILVIUS, A.J.G. (2011) The Business Value of IT: A Conceptual Model for Understanding and Selecting Valuation Methods. In N. Shi, & G. Silvius (Eds.), Enterprise IT Governance, Business Value and Performance Measurement. Hershey, PA.

2011:109

SOANES, C., STEVENSON, A. EDS. (2008) The Concise Oxford English Dictionary. Twelfth edition. Oxford Reference Online. Oxford University Press. Rhodes University Library. 28 September 2008

STANDISH GROUP (2011) The CHAOS manifesto. The Standish Group International. 2011

STENZEL, J. (ED.) (2007) CIO Best Practices. John Wiley and Sons, Inc. Hoboken, New Jersey. 2007

STEVENS, F. (2011) Frameworks for IT Governance Implementation. In N. Shi, & G. Silvius (Eds.), Enterprise IT Governance, Business Value and Performance Measurement (p16). Hershey, PA. 2011:16

SUTER, R. (2007) Securing strategic benefit from enterprise architectures. Defense AT&L. January-February 2007:20

SYMONS, C. (2008) IT governance for the new ecosystem. Forrester Research, Inc., 2008:4

SYMONDS, C. (2009) Governance Communications - Measuring And Improving Governance With A Balanced Scorecard, Forrester Research, Inc., 6 February 2009

US SECURITY AND EXCHANGE COMMISSION (2002) http://www.sec.gov/about/laws/soa2002.pdf, accessed 16 December 2013

VIOLINO, B. (2006) Knowledge center security. Computerworld. April 17, 2006.

WARD, M. (2011) Technology Partner Governance. In N. Shi, & G. Silvius (Eds.), Enterprise IT Governance, Business Value and Performance Measurement. Hershey, PA. 2011:244

WHITE, T. (2001) Reinventing the IT department. Oxford: Butterworth-Heinemann. 2001:292

WILKINSON, J. (ED.) (2008) Service Strategy Based on ITIL V3 – A Management Guide. Van Haren Publishing, Zaltbommel. June 2008

# Appendix One – Original Participant Disussion Draft

# DRAFT DISCUSSION PAPER ON

# *FORMULATING AN IT GOVERNANCE FRAMEWORK*

## In Support of Master of Commerce Dissertation

## at Rhodes University

**Author: Pieter Roos (Student number 08R6759)**

**December 2010**

# TABLE OF CONTENTS

### IT Governance Structure Recommendations

Office of the CIO – Recommendation 21
Chief Technology Officer – Recommendation 22
Information Security Officer – Recommendation 23
Chief Enterprise Architect – Recommendation 24
IT Financial Manager – Recommendation 25
IT Risk Officer – Recommendation 26
Applications Manager – Recommendation 27
Technical Manager – Recommendation 28
Operations Manager – Recommendation 29
IT Strategy Committee – Recommendation 30
IT Steering Committee – Recommendation 31
Enterprise Architecture Forum – Recommendation 32
Programme Management Office – Recommendation 33
Summarised Recommendation on IT Governance Roles – Recommendation 34
Summarised Recommendation on IT Governance Structures – Recommendation 35

## *APPENDIX B – STRUCTURED INPUT SCHEDULE*

# 1. Introduction

## 1.1 Background

This discussion paper serves as the basis for sourcing feedback from ten Chief Information Officers (CIOs) of large (annual revenue in excess of R1bn for private sector companies or budget in excess of R1bn in the case of government organisations) South African organisations, in support of a Master of Commerce thesis on Information Technology (IT) governance, titled "Formulating an IT Governance Framework".

## 1.2 Objectives

The objectives of the feedback based on this discussion paper are to:

- Validate and update the proposed framework to arrive at a generic IT governance framework that is relevant to all the organisations interviewed; and
- Identify IT governance trends across the organisation interviewed.

## 1.3 Scope

This paper describes a proposed IT governance model that covers the following:

- Roles and structures for effective IT governance;
- Enablers for IT governance;
- Major IT governance processes; and
- Discussion and critique of a proposed generic IT governance framework, covering specifically:
    - Relevance of the framework and its practicability at each organisation; and
    - Potential improvements to the proposed framework.

## 1.4 Scope Exclusions

General business processes that are not IT specific are not covered explicitly, including:

- Corporate strategy;
- Physical security;
- Enterprise portfolio, programme and project management (only included for IT);
- Business continuity management;
- Supply chain management and the corporate procurement function;
- Enterprise risk management (only IT risk management as a sub set is included in the scope); and
- Corporate performance management (only IT performance management as a sub set is included in the scope).

## 1.5 How to Use this Paper

The participants are requested to respond as follows:

- Carefully read this discussion paper (pages 5 to 21; it is suggested that these pages are printed and cross-viewed during feedback generation);
- Use appendices A and B to provide your feedback:
    - In each of the yellow-shaded comment areas, provide your feedback; and
    - Email appendices A and B, with your comment, to pieter@itgovpartner.com.

## 2. Proposed Framework

The working definition of an IT governance framework adopted for this paper is, "the underlying structure supporting IT governance through the combination of governance structures, architecture, processes, desirable practices and an IT control framework to effectively support the IT governance major processes".

According to this definition, the components making up the "underlying structure" or framework are:

- Processes: The five IT governance major processes are broken down into sub processes modelling all aspects of the IT environment. All governance structures, desirable practices and IT controls map back to the major processes, while the processes map back to the enterprise architecture;
- Governance structures: These are the roles, positions, governing bodies and structures overseeing IT governance in the organisation;
- Architecture: This is the IT component (IT architecture) of the enterprise architecture, which reflects the composition of the organisation and the alignment of all architectural elements to organisational objectives;
- Desirable practices: The definition formulated in the Introduction to this dissertation is, "the most appropriate practice accepted by consensus as a de facto standard or through certification as a de jure standard". More specifically, this research takes an interest in desirable practices supporting IT governance; and
- IT control framework: In the Introduction to the dissertation, the definition provided was "the underlying structure of the IT internal control environment, including all the most significant (or key) controls for the IT environment, together with the complementary, supporting (or non key) controls".

To facilitate a structured, logical approach to constructing a generic framework, the researcher summarised the five components mentioned above into the three dimensions of Diagram 1, viz.

- The IT governance major processes have been taken from the IT Governance Institute's model and represent the high-level processes that form the backbone of the framework and are used as the focal integration point of the IT governance framework. The major processes specify "what" should be done to practise sound IT governance, more specifically IT risk management, performance management, strategic alignment, resource management and performance management;

- Enablers for IT governance include the sub processes, architecture and control framework, all based on desirable practice, enabling the IT governance major processes. If the major processes are considered the backbone, the enablers are the muscles producing motion. The enablers are the embodiment of day-to-day IT governance and specify "how" sound IT governance should be practised; and
- The roles and structures for effective IT governance are the main roles and bodies for effective IT governance. The IT governance structures specify "who" all is responsible and accountable for the effectiveness of the sub processes making up the five IT governance major processes.

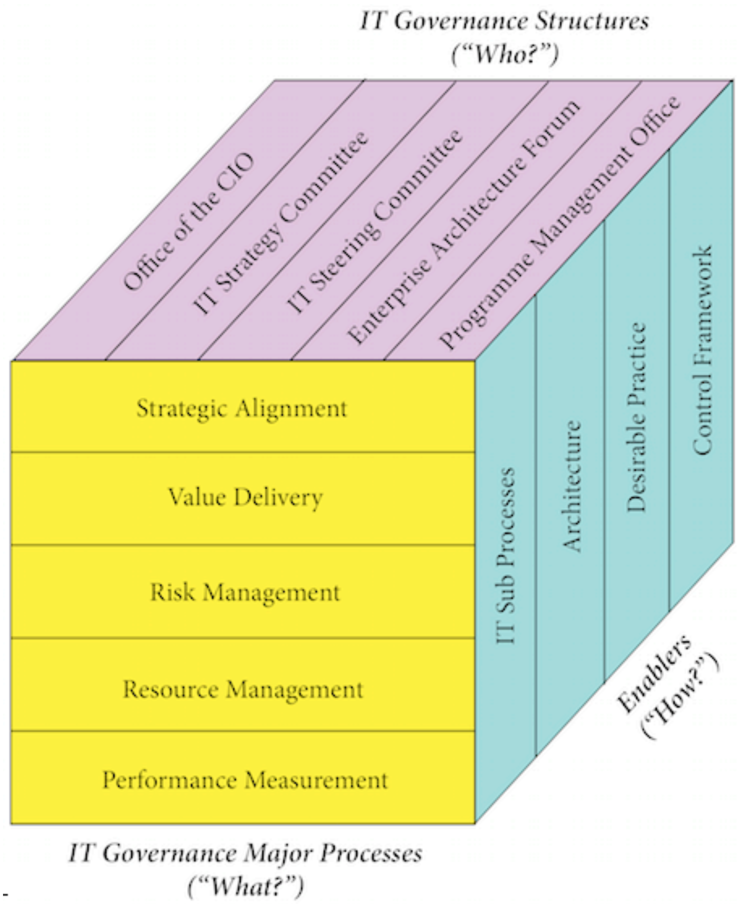


**Diagram 1 –PES IT Governance Framework**

There are arguments towards the fact that no universal framework exists that provides a single, cohesive view of all aspects of IT governance that is appropriate for most large organisations. The Processes, Enablers and Structures (PES) IT governance framework depicted in Diagram 1 provides such a single, cohesive view that could be populated to serve as a generic framework suitable for any large IT function.

The cube depicted in Diagram 1 was designed by the researcher for use as the basis for consulting on IT governance over the past five years. The discussion paper is structured around the three dimensions of the cube and covers all of its components in Section 3 below.

## 3. Major Process Overview

The proposed structures and enablers should all be viewed in the context of the five major processes, which are described below. The recommendations related to each process are made in Appendix A.

### 3.1 Strategic Alignment (Recommendation 1)

Strategic alignment requires IT objectives (and accordingly the IT strategy), IT operations and investment in IT to support the achievement of organisational objectives. In its most basic form, strategic alignment of IT to organisational objectives starts with IT strategic planning. Enterprise architecture and IT portfolio management provide valuable mechanisms for aligning IT to business. Enterprise architecture is considered a means of ensuring that structures, processes, systems and infrastructure are aligned to organisational objectives, while IT portfolio management is considered to support the alignment of projects and services to organisational objectives.

Bodies involved in monitoring the strategic alignment of IT include the Enterprise Architecture Forum, the IT Strategy Committee and the IT Steering Committee. In the IT context, sound governance requires the alignment of IT strategy, planning, investment and operations to technologically enable departments contributing to strategic objectives. This is achieved by implementing a performance management process, which includes the formulation of IT objectives with related key performance indicators (KPIs) that make it clear how IT would enable these departments to achieve their objectives.

### 3.2 Value Delivery (Recommendation 2)

The focus of value delivery is on return on investment (ROI) , i.e. does the investment in IT yield the return expected at the point of committing to the investment?

The ValIT Framework, originally published by the IT Governance Institute during 2006, provides a useful structure for value delivery, comprising value governance, portfolio management and investment management. ValIT is still relatively new and few South African organisations have adopted it, but long-term IT governance frameworks cannot afford to ignore it.

An important mechanism for delivering value is the service level management process, which manages and monitors service delivery in accordance with the service strategy and design. Service level management is a service delivery process, included in the IT Infrastructure Library (ITIL).

As a vehicle for facilitating value delivery, the Programme Management Office (PMO) is a structure that translates IT strategy into execution. Where IT organisations are most successful at delivering value, IT governance practices are often embedded within broader corporate governance. This manifests in areas such as project portfolio management, where the enterprise and IT processes are aligned or formally integrated.

Sometimes overlooked as a value delivery enabler, enterprise architectural competency presents a critical part of value delivery.

## 3.3 Resource Management (Recommendation 3)

COBIT identifies four IT resource categories, including applications, information, people, and infrastructure. COBIT, as a recommended practice for IT internal controls, is discussed in the Enablers section below.

Formal IT processes are required to manage these resources and are supported by policies, procedures, standards, methodologies and an internal IT control framework. To formalise IT processes within the operational COBIT domains, the desirable practices discussed in the Enablemers section should be applied.

Specific enablers supporting resource management are IT service management, project management (monitored via a PMO) and information security management. The management roles identified in the IT Governance Structures section are the ones responsible for resource management.

## 3.4 Risk Management (Recommendation 4)

IT risk management focuses on three processes, namely: Risk Governance, Risk Evaluation and Risk Response, in order to:

- Set responsibility for IT risk management;
- Set objectives and define risk appetite and tolerance;
- Identify, analyse and describe risk;
- Monitor risk exposure;
- Treat IT risk; and
- Link with existing guidance to manage risk.

The RiskIT exposure draft is the IT Governance Institute's first step in establishing a formal directive on IT risk management, as a complementary publication to COBIT and ValIT. RiskIT provides a mapping between COBIT and the IT risk management process.

The traditional view of IT risk management has often emphasised information security management and IT service continuity management. When comparing RiskIT, ITIL (specifically the IT Service Continuity Management Process) and ISO/IEC27001 (Information Security Management Process) it becomes clear that more or less the same process could be followed for identifying and analysing risk pertaining to any aspect of IT.

Most IT risk management programmes are not aligned to enterprise risk management. Effective IT risk management is only possible as a sub set of the overall enterprise risk management process. Conversely, all line managers who rely on IT should contribute to IT risk management.

### 3.5 Performance Measurement (Recommendation 5)

Performance measurement monitors strategy implementation, project completion, resource usage, process performance and service delivery. Balanced scorecards monitor the translation of strategy into action. The IT Governance Institute proposes the implementation of an IT balanced scorecard incorporating the following perspectives:

- Enterprise contribution – How do business executives view IT?
- User orientation – How do users view IT?
- Operational excellence – How effective and efficient are the IT processes?
- Future orientation – How well is IT positioned to meet future needs?

The Balanced Scorecard paragraph in the Enablers section discusses this mechanism and should be referenced for more details on performance measurement.

## 4. Enabler Overview

The proposed enablers required to implement a generic IT governance framework are described below.

### 4.1 ITIL (Recommendation 6)

ITIL represents desirable practice for Service Management and the complete service lifecycle, from service strategy through to service operation, including all aspects of service support and service delivery.

The IT Governance Global Status Report – 2008, issued by the IT Governance Institute, shows that ITIL is considered the most referenced practice influencing IT governance frameworks.

Prior to the latest publications that were released in 2007, the most widely known ITIL publications were the Service Support and Service Delivery modules, which cover the following processes:

- Service Support: Configuration management, change management, release management, incident management, problem management and the service desk function.
- Service Delivery: Service level management, financial management for IT services, capacity management, IT service continuity management, and availability management.

In ITIL Version 3, the Service Support and Service Delivery publications were not replaced, but updates are expected to follow.

The 2007 ITIL 3 update introduced five complementary titles, namely: service strategy, service design, service transition, service operation, and continual service improvement.

## 4.2 COBIT (Recommendation 7)

Since its birth in the late 1990s, COBIT has, at the time this research was conducted, matured into COBIT 4.1. According to the IT Governance Global Status Report– 2008, it is the second most referenced among frameworks considered to be influencing IT governance and is unique as a commonly available, non proprietary, framework of IT control objectives.

COBIT adopts a generic view of the IT environment, breaking it down into 34 processes that are grouped into the four domains of Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. Each of the 34 processes is broken down into control objectives that are classified according to resource types impacted (applications, information, infrastructure or people), business requirements (effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability), and IT governance major processes impacted. To facilitate formal process design, each process also has a suggested list of inputs from and outputs into other processes, a RACI chart summarising responsibilities and accountabilities for roles related to the process, goals and metrics, and suggested maturity ratings.

## 4.3 The ISO/IEC27000 Family of Standards (Recommendation 8)

The ISO/IEC27000 series currently includes ISO/IEC27001, which specifies the requirements for establishing an information security management system and 27002, which has absorbed ISO/IEC17799.

In its third version, ITIL now provides guidance on the security management process as it relates to all other operational IT processes. As such, ITIL V3 is an important complement to ISO/IEC17799 and ISO/IEC27001 for managing information security.

The ITIL Information Security Management Process provides a security framework, information security policy and guidance for implementation of the ISO/IEC17799 security management system.

## 4.4 Balanced Scorecard (Recommendation 9)

In the early nineties, Robert Kaplan and David Norton coined the term, "Balanced Scorecard" (Kaplan, 1996:viii), a term that has since become widely used in corporate performance measurement circles. "The Balanced Scorecard provides executives with a comprehensive framework that translates a company's vision and strategy into a coherent set of performance measures (Kaplan 1996:24)."

The balanced scorecard is "a carefully selected set of quantifiable measures derived from an organisation's strategy" (Niven, 2006:13). Many variants of the original balanced scorecard exist, though are all based on the initial concepts articulated by Norton and Kaplan (Olve, 2006:15).

The balanced scorecard provides an effective framework for implementing governance communications, based on its focus on strategic alignment, its perspective beyond financial measures, and its combination of leading and lagging metrics (Symonds, 2009:4).

## 4.5 Prince2 and PMBOK (Recommendation 10)

Prince2 provides a structured method for effective project management, whereas PMBOK is the definitive work on project management standards. As such, it complements PMBOK well, providing the "how", while PMBOK states the "what". The current edition of Prince2 was released in 2005, with an update expected in 2010.

Prince2 defines a project management method, providing a framework for the wide variety of project disciplines and activities. It focuses on the business case, which drives all project management processes, from initiation to conclusion.

Considering the findings of the IT Governance Global Status Report – 2008, PMBOK and Prince2 are considered project management-related desirable practice.

PMBOK is the definitive work on project management standards. It published by the Project Management Institute and provides general guidance on all aspects of project management, including integration, scope, time, cost, quality, human resources, communication, risk, and procurement management. Prince2 provides a structured method for effective project management (Office of Government Commerce, 2005:1), i.e. meeting the standard defined by PMBOK.

## 4.6 TOGAF (Recommendation 11)

The Open Group Architecture Framework provides a generic enterprise architectural framework to a wide community in a similar way the Open Source Movement supports sharing of software.

In its list of frameworks influencing IT governance, the IT Governance Global Status Report – 2008 (IT Governance Institute, 2008:36) only included TOGAF as an architecture framework. Even though it was not referenced by that many organisations, it still made the list.

With the increasing number of publications such as ITIL advocating a services orientation, organisations might do well to consider the suitability of adopting a service-oriented architecture, which makes services available in a transparent manner.

Enterprise architecture aspects, as far as the roles of the chief enterprise architect and the Enterprise Architecture Forum are concerned, are discussed in the IT Governance Structures section.

## 4.7 VALIT (Recommendation 12)

The ValIT Framework, originally published by the IT Governance Institute during 2006, provides a useful structure for value delivery, comprising value governance, portfolio management and investment management.

ValIT is a unique publication in IT. With all the effort devoted to its development, this framework is already in its second release. The precedent set by COBIT appears to be a positive indicator that the IT Governance Institute might have similar success with ValIT.

ValIT is still relatively new and few South African organisations have adopted it, but long-term IT governance frameworks cannot afford to ignore it.

The framework is still developing and needs to be promoted more widely before it will gain wide acceptance.

## 4.8 King III Report (Recommendation 13)

The past two years saw two significant publications that no listed South African company or government organisation can ignore in its approach to practising IT governance. The King Report on Governance for South Africa 2009 (“King III”) has become an important requirement for the larger players in corporate South Africa, while over the longer term, the first international standard on IT governance, ISO/IEC38500, is likely to become the global reference on IT governance fundamentals.

Any generally accepted generic IT governance framework will have to incorporate the principles of these two publications in order to ensure its long-term relevance.

King III is relevant to all South African companies, specifically those listed on the Johannesburg Stock Exchange. New listing requirements and potential future corporate financial reporting standards are expected to contain a statement of compliance with King III, which now includes a section dedicated to IT governance.

## 4.9 ISO/IEC38500 (Recommendation 14)

ISO/IEC38500 provides organisations with six principles for the effective, efficient and acceptable use of IT in their organisations. It is the first formal ISO standard on IT governance. The standard sets out six principles for "good corporate governance of IT", which deal with allocation of responsibility, IT strategy, making acquisitions with business value in mind, IT performance to the agreed service levels, conformance with legislation and regulations, and respect for human behaviour or "the people in the process".

The standard follows and globalises the related, pioneering Australian standard AS-8015 Corporate Governance of Information and Communications Technology, and is likely to be accepted and implemented globally.

At this stage the standard is still limited to a set of principles and does not include detailed guidance on their implementation.

## 4.10 IT Sub Processes (Recommendation 15)

The IT governance major processes provide the five broad process classes, which require IT sub processes within each class. For an effective internal control environment that supports corporate governance, information technology controls need to mature to a level where they could be relied upon to preserve the confidentiality, integrity and availability of information assets.

As a prerequisite to an effective system of internal IT control, however, it is necessary to raise IT sub process maturity to a level where controls could be embedded firmly in the process. Low process maturity complicates control over processes and could increase the cost of implementing controls.

Control design is driven by risk assessments and is captured in an IT control framework, which is translated into policies, procedures, standards, and methodologies to implement the required governance mechanisms.

Enabling components are broken down into policies, procedures, standards, methodologies, and risk assessments.

COBIT 4.1 incorporates process maturity classifications and metrics into the COBIT framework for their use during process formalisation and improvement initiatives. It represents a desirable practice for IT control objectives and a common point of reference for IT professionals and auditors alike.

Adopting a COBIT view of the IT environment, 34 processes are distinguishable, which COBIT maps back to the five IT governance major processes, linking the "what" and "how" dimensions of the cube in Diagram 1.

## 4.11 IT Control Framework (Recommendation 16)

The IT internal control component represents a significant part of IT governance. It maps the IT internal control environment to the IT risk register, indicating how risks will be mitigated, transferred or avoided.

IT controls provide the integrity layer protecting IT business processes. COBIT is the most widely accepted set of control objectives used as the basis for formulating IT controls, but other sources also provide more specific, specialised control objectives, such as those for information security, published under ISO/IEC27000.

## 4.12 Supporting Documents (Recommendation 17)

The documents "legislating" IT governance in the organisation include policies, standards, procedures and risk assessments.

IT policies lay down the principles that influence and guide the execution of IT procedures and the application of IT standards in line with the philosophy, objectives and strategic plans established by the Office of the CIO. They also describe the consequences of non-compliance with the principles they define. Good policies clearly assign roles and responsibilities, explain the rules that should be enforced, along with their enforcement mechanisms, and clarify desirable vs. non desirable behaviour. Being the owner of these documents, the CIO is accountable for the maintenance and overall enforcement of all IT policies and standards across the organisation.

Standards and procedures explain the detail for implementing policies, which are more high-level by nature.

The mandatory requirements of individual policies are set out in standards, which describe the desirable outcome of processes and sometimes the minimum configuration requirements for specific technologies, or the minimum performance requirements for specific actions, in support of policies and procedures.

Procedures describe the detailed actions to successfully complete a task, i.e. the process flows for executing IT processes. These procedures belong to the heads of the various IT departments, who are also responsible for the customisation, implementation and maintenance of IT procedures for their individual departments.

Risk assessments involve management identifying and analysing relevant risks that could prevent IT from achieving its objectives, as a basis for the design of controls making up the IT control framework.

### 4.13 Architecture (Recommendation 18)

The enterprise architecture consists of four parts, namely: the business, information, application, and technical architecture layers.

Enterprise architecture is an important mechanism for integrating IT and the business. Architecture is covered under the *TOGAF* sub paragraph and the role of the chief enterprise architect.

It is an area that is still in an early stage of maturity at most South African companies, which might make a decision on the adoption of enterprise architecture frameworks premature, however, organisations need to start exploring this area and the available tools.

### 4.14 Portfolio Management (Recommendation 19)

"IT portfolio management assesses the impact of existing IT activities, and provides tools to assess the value of future IT investments. For IT professionals, this brings visibility and rigor to the review and planning processes (Caruso, 2007:49)."

Portfolio management is a developing which authors view in a number of different ways.

The ValIT Framework (IT Governance Institute, 2008), first published by the IT Governance Institute during 2006, provides a useful structure for value delivery and covers portfolio management as one of its three focal areas.

As part of its extension, ITIL V3 has added the Service Portfolio Management process, which aligns IT services to business (Office of Government Commerce, 2007:119).

## 5. IT Governance Structure Overview

The proposed roles and structures to implement a generic IT governance framework are described below.

### 5.1 Office of the CIO (Recommendation 21)

Over the past two decades, the role of the CIO has largely focused on deploying IT and controlling costs, however, the CIO's role should be one that is business oriented, rather than a technically oriented role in order to act as a bridge between IT and the rest of the organisation. Modern CIOs are not only expected to have extensive IT experience but also depth in business and industry.

This section considers four roles traditionally associated within the office of the CIO, namely: the information security officer, chief enterprise architect, IT financial manager, and IT risk officer. These are not necessarily full-time positions but areas of responsibilities that are assigned by the Office of the CIO.

New roles being defined for the Office of the CIO include the following:

- IT planning manager – responsible for the creation and maintenance of IT planning, communication of business needs to IT, and education of stakeholders in business on what the IT organisation can do for the business;
- IT programme management office manager – responsible for the effective delivery of the portfolio of IT projects; project monitoring and reporting; and, by implication of IT project governance, maintaining project management standards; and
- IT vendor manager – responsible for managing IT suppliers and the relationship with them, collaborating with business and IT to set sourcing strategies and define vendor oversight processes. This roles requires a procurement expert who is responsible for monitoring IT vendor viability, especially as far as security and disaster recovery are concerned.

As these three roles have not yet matured and become general practice in IT organisations, they are not included as generic roles in a generic IT governance framework.

## 5.2 Chief Technology Officer (Recommendation 22)

The CTO considers the appropriateness of technology acquisitions in view of the IT and organisational strategies, focusing on effectiveness (doing the right things) and efficiency (doing things right). In an organisation where the CTO assumes a technical, engineering role, this role might reside outside the IT department. The CTO role is justified on an organisation-by-organisation basis, depending on the needs and culture of the organisation. It is not a standard role to be found in all IT environments. Some organisations combine the CIO and CTO roles, although in a highly technical engineering or telecommunications environment that might not be possible.

## 5.3 Information Security Officer (Recommendation 23)

The Information Security Officer (ISO) is responsible for formulating information security policies, procedures and standards aligned to international standards and practice, e.g. ISO/IEC27000, and for monitoring compliance with approved security policies, procedures and standards.

Although no de facto standard for the role of information security manager exists, ISACA identifies five job practice areas for ISOs, namely: information security governance, risk management, information security programme development, information security programme management, and incident management and response.

Information security management represents a key area of IT governance to the extent that some people even wrongly believe it to be the only important area on this topic. It requires a significant level of skill and expertise often not found in other roles.

## 5.4 Chief Enterprise Architect (Recommendation 24)

The enterprise architecture represents the organising logic for business process and IT infrastructure and reflects the integration and standardisation requirements of the company's operating model. It provides a long-term view of a company's processes, systems and technologies so that individual projects can build capabilities.

The chief enterprise architect segregates the enterprise architecture layers and outlines the architecture of each layer, formulates architectural standards and monitors compliance with these standards, while the Enterprise Architecture Forum oversees the definition of architectural standards, alignment of the IT organisation with organisational objectives and the maintenance of architectural integrity, as well as instituting action against parties that do not comply with architectural standards.

The chief enterprise architect focuses on the alignment of corporate strategy to the processes and systems of the enterprise. He or she also facilitates and encourages compliance with standards for the organisation, considering both strategy and project execution for the achievement of strategy. In some organisations, the chief enterprise architect reports into a business portfolio, sometimes even the CEO, but usually this role reports directly to the CIO.

This paper identifies the chief enterprise architect as important to the effectiveness of the Extended IT Organisation. As shown in the Enablers section, enterprise architecture is still a young, evolving function. For that reason it is not possible to determine the optimal reporting line, i.e. whether the chief enterprise architect should report into the Office of the CIO or into another business function such as Corporate Strategy. Considering the fact that current awareness of this role is strongest in IT in most organisations, the role in its current form would probably be retained in IT, which is the position adopted by this research. Regardless of the choice of reporting line, a principle that should be adhered to is that the IT architecture role cannot be outsourced.

## 5.5 IT Financial Manager (Recommendation 25)

IT financial management is a role that could justify a full-time position in many large IT organisations, but it could also be a support function provided by the finance department. It involves the following responsibilities:

- Overseeing the capital and operational IT budgeting process and monitoring actual vs. budgeted IT expenditure;
- Depending on the maturity of the organisation, costing of IT services per the service catalogue to the various end-user departments, and, if required by policy, charging these costs back to the individual departments;
- Monitoring compliance of IT procurement with organisational policies and procedures, and with IT hardware, software and service standards; and
- Monitoring IT programme spend at the portfolio level.

## 5.6 IT Risk Officer (Recommendation 26)

Many publications exist on enterprise risk management and its direct sub processes, yet few comprehensive works have been published on the IT risk management specialisation, apart from the recently published Risk IT exposure draft.

Risk IT defines the IT risk management process model in three domains, namely: Risk Governance, Risk Evaluation and Risk Response. It assigns accountability for IT risk management to the chief risk officer, but makes provision for the creation of an IT risk officer role.

## 5.7 Applications Manager (Recommendation 27)

The applications manager is responsible for managing applications through their lifecycle. He or she could play a significant role in systems development, although that is not a prerequisite.

The applications manager is the custodian of technical application management knowledge and expertise and provides the balance between the cost and skills level of application management staff. He or she also provides the resources to support the IT service management lifecycle and integrates the Application Management Lifecycle into the IT Service Management Lifecycle.

The applications manager guides IT operations on ongoing operational management of applications.

Taking a broad view on the role of the applications manager, he or she is also responsible for:

- Monitoring the performance and operation of applications, whether batch or online, real-time;
- Application data integrity;
- Application performance tuning;
- Application patch management; and
- Monitoring application integrity, i.e. ensuring that the change and release and deployment procedures are complied with as far as applications are concerned.

## 5.8 Technical Manager (Recommendation 28)

The technical manager is the custodian of technical knowledge and expertise related to managing the IT infrastructure. This role resources the technical infrastructure supporting the IT service management lifecycle, from service design through service operation and continual technology improvement. The technical manager is also responsible for guiding the operations manager on ongoing operational management of technology.

It cannot be dictated whether the technical manager or the applications manager owns and is responsible for the IT Service Support and IT Service Delivery processes, but it is required that these two roles take responsibility for Service Support and Service Delivery between themselves.

## 5.9 Operations Manager (Recommendation 29)

In a large IT environment, the number of operations staff and sometimes the number of facilities warrant the appointment of an operations manager.  This usually depends on the size of the department.

The operations manager is responsible for:

- Operations control, including console management, job scheduling, backup and restoration, print and output management, recording and monitoring operational logs, and maintenance activities on behalf of application and technical management;
- Maintaining shift and operations schedules, managing and resourcing operational shifts, and maintaining reports on operational activities;
- Managing the physical environment (facilities), including data centres and recovery facilities, and, where required, managing consolidation of facilities;
- Maintaining and managing standard operating procedures, and ensuring compliance with operational service and infrastructural standards to maintain a stable operating environment; and
- Responding to business needs for scaling infrastructural capacity to levels that effectively support continually changing or expanding IT services.

## 5.10 IT Strategy Committee (Recommendation 30)

The IT Strategy Committee is a board-level committee, composed of Board members and non-Board executives, including the CIO.  It assists the Board in governing and overseeing the enterprise's IT-related matters. It should ensure that IT governance is addressed formally and that the Board has the information it requires to ensure effective governance over IT.

The Committee concerns itself with the alignment of IT to organisational objectives, more specifically, how IT delivers against strategy, how IT investments support the current and future needs of the organisation, and focusing IT on specific organisational objectives that are dependent on IT enablement.

## 5.11 IT Steering Committee (Recommendation 31)

The IT Steering Committee is at the executive level and focuses on tracking IT investment, setting priorities for IT and allocating scarce IT resources.  It typically combines senior business executives and IT management, with its membership often being indicative of the view of IT value in the organisation.  Contextualising the 2003 view of the IT Governance Institute with developments since, its role could be equated to that of an IT Portfolio Management Committee, as most of the responsibilities assigned to it by the IT Governance Institute map onto the IT Portfolio Management process.

The Committee meets regularly to provide direction and oversight for IT across the enterprise. The IT Steering Committee is closely associated with IT service and project governance, and provides guidance and oversight for all other IT Steering Committees, and governs strategic functions including architecture, planning and vendor management.

Luftman (2004:303) takes a different perspective, reducing the role of the IT Strategy Committee to setting the long-term IT strategy and stating that the IT Steering Committee business has the role of IT in the organisation, aligns IT with business, establishes IT investment principles, and sometimes establishes architectural principles and guidelines. This allocates most of the IT Governance Institute's view of the IT Strategy Committee to the IT Steering Committee.

## 5.12 Enterprise Architecture Forum (Recommendation 32)

As part of the Extended IT Organisation, the Enterprise Architecture Forum focuses on the structure of the Extended IT Organisation and how it relates to the organisation overall.

Top management, together with IT leadership, are responsible for establishing general enterprise architecture principles, while middle management and IT are responsible for enterprise architecture policy directives. The architecture function itself is responsible for developing appropriate architecture models. The Enterprise Architecture Forum is the body for achieving just that.

## 5.13 Programme Management Office (Recommendation 33)

The IT PMO oversees the execution of programmes and projects in fulfilment of the strategic objectives of IT, as a sub set of the wider portfolio of projects in the organisation. The PMO also develops and enforces programme and project standards, reports on progress and assists in obtaining approval of project budgets.

The IT PMO reports to the Enterprise PMO (EPMO), whose influence extends beyond one business unit or functional area. In some organisations, IT programmes and projects are driven by the EPMO, while others create an IT PMO for that purpose. As long as both apply strong programme and project management principles and follow consistent methodologies, there is little difference between the two approaches.

At the enterprise level, the portfolio management process aligns programmes (collections of projects with shared objectives) to organisational objectives. Diagrammatically, this could be depicted by three concentric circles, with the innermost circle representing projects, the middle circle programmes, and the outer circle portfolios of programmes.

## 6. Conclusion

The PES Framework presented in this paper provides a single, cohesive view of all aspects of IT governance that is appropriate for most large organisations.

By following the recommendations of the paper, the framework supports the implementation of customised processes, enablers and structures required for effective IT governance in the various organisations involved in this research. Such an implementation could be tailored to focus on specific compliance objectives under, for example, a King III or ISO/IEC38500 project.

The input provided by the various CIOs has contributed to the outcome of this research being more representative of the needs of the South African IT community, and reflecting practical recommendations for implementing IT governance processes, enablers and structures.

# APPENDIX A – (RECOMMENDATION AND COMMENT SCHEDULE)

## General

**Participant comment**

## IT Governance Major Process Recommendations

### Strategic Alignment – Recommendation 1

- Organisations should have a formal IT strategy that is aligned to organisational objectives and that is updated at least annually;
- IT services should be aligned to the IT strategy, either informally or through formal enterprise architecture and service portfolio management mechanisms;
- Enterprise architecture and IT portfolio management should be considered as mechanisms for aligning IT and organisational strategies;
- An IT Strategy Committee or a combined IT Steering and Strategy Committee should be instituted to oversee the alignment of the IT strategy to the organisational strategy; and
- The establishment of an Enterprise Architecture Forum should be considered.

**Participant comment**

### Value Delivery – Recommendation 2

Recognising that ValIT is a relatively new framework and that formal value delivery is still in its early stages of maturity, it is recommended that a formal service level management process be adopted for defining value measurement criteria around key services, and that consideration be given to how ValIT could be used in support of value delivery in future. It is also recommended that:

- The service level management process be formalised to closely monitor value delivery at the operational level;
- A programme management office be established to monitor significant IT projects; and
- The role of enterprise architecture be considered as an enabler of value delivery.

**Participant comment**

### Resource Management – Recommendation 3

It is recommended that the official organisational processes for resource management be practised in IT and that specific processes be implemented for IT service management, project management (monitored via a PMO) and information security management.

**Participant comment**

### Risk Management – Recommendation 4

It is recommended that a comprehensive IT risk identification and assessment process be implemented, as well as a formal IT control framework indicating the approved responses to all significant IT risks. The Risk IT framework is still an early draft publication to complement COBIT and ValIT, but its development should be monitored to ensure that any future value that may be derived from it is not overlooked.

IT risk management should also be integrated with the enterprise risk management process.

**Participant comment**

### Performance Measurement – Recommendation 5

It is recommended that a formal IT performance measurement process be implemented, whether in balanced scorecard fashion or using any other proven method.

**Participant comment**

## Enabler Recommendations

### ITIL – Recommendation 6

It is recommended that ITIL or a branded version of it, such as the Microsoft Operations Framework, be used when formulating IT service strategy, design, operation and general IT service management processes, implementing a security management system as described by ISO/IEC27000, or when designing IT/business alignment mechanisms. ITIL supports the Value Delivery, Resource Management, Risk Management and Strategic Alignment major processes. ISO/IEC20000 is only recommended for organisations striving to achieve international ITIL certification. It does not directly support the proposed IT governance framework. The COBIT Delivery and Support processes, and change and release management processes from the Acquisition and Implementation domain, directly support ITIL.

**Participant comment**

### COBIT – Recommendation 7

COBIT 4.1 provides a comprehensive set of IT control objectives supporting the organisation's IT control framework, a high-level IT process map and an IT process maturity benchmark through its CMMI process maturity model. COBIT supports all five of the IT governance major processes. In terms of a proposed IT governance framework it is recommended that the 34 processes proposed by COBIT 4.1 be prioritised and that the following be done for each key (high priority) process:

- A procedure be adopted to serve as the minimum level of formalisation of the process and as the basis for a consistent approach to the process;
- Where possible, desirable practice should be followed;
- Process maturity should be graded, using the CMMI grading included per COBIT 4.1 process;
- Key controls be defined and implemented for the process, and staff trained on the effective use of each control; and
- Input from internal and external audit sought on the design effectiveness of key controls.

**Participant comment**

### The ISO/IEC27000 Family of Standards – Recommendation 8

ISO/IEC27000 (including ISO17999) represents desirable practice for information security management systems and control guidance. It is recommended that organisations that have achieved a level four COBIT 4.1 process DS5 CMMI maturity consider formally implementing ISO/IEC27000. However, all organisations would benefit from consulting the control objectives and controls proposed by ISO/IEC27000, when implementing process DS5. ISO/IEC27000 should be considered in support of the Risk Management IT governance major process. ITIL supports aspects of the security management system promoted by ISO/IEC27000.

**Participant comment**

### Balanced Scorecard – Recommendation 9

Organisations are encouraged to consider the balanced scorecard as a performance measurement mechanism, but should adopt some performance measurement tool to address the IT governance major process, Performance Measurement, in the generic framework.

**Participant comment**

### Prince2 and PMBOK – Recommendation 10

As the definitive work on project management, it is recommended that PMBOK be used as the project management standard for organisations adopting the generic IT governance framework, with a project management method such as Prince2 for comprehensive project management processes. PMBOK supports the Strategic Alignment major process; more specifically, COBIT process PO10. Organisations have a number of project management methods, so any structured method could be used if Prince2 is not adopted.

**Participant comment**

### TOGAF – Recommendation 11

It is recommended that organisations explore ways of formalising their enterprise architecture (EA) through the use of frameworks like TOGAF and the work of Weill and Ross. EA is a growing, maturing field and, at this stage, there is no clear, single answer. EA supports the Strategic Alignment major process.

**Participant comment**

### VALIT – Recommendation 12

It is recommended that the Value Delivery major IT governance process be implemented using ValIT, to formalise value management practices and align IT portfolio management to corporate portfolio management processes.

**Participant comment**

### King III Report – Recommendation 13

Where the organisation has decided to implement the recommendations of the King III report, it is suggested that the following be implemented to fulfil the requirements of the IT governance chapter of King III:

13.1 A Board IT governance awareness programme be undertaken to ensure the directors understand all aspects of IT governance, for which they are accountable.

13.2 An IT charter be established, setting out the objectives of the IT function in support of organisational objectives, including sustainability objectives, and governance requirements of the IT function. The charter should also define all key IT governance structures and roles, and their decision-making responsibilities and accountabilities.

13.3 A set of policies, procedures and standards be implemented to guide behaviour in IT, in line with the IT charter.

13.4 A formal IT risk management function be implemented, with the CIO accountable for effective IT risk management and a specific person responsible for ensuring compliance with the required IT risk management practices. Under this process a formal IT risk register should be implemented.

13.5 An IT internal control framework be implemented, to match the IT risk register. The controls should be designed to clearly specify what actions are to be undertaken, at what frequency, by whom, and what evidence of executing these actions should be retained.

13.6 IT be awarded a dedicated section of the integrated report required by King III, with regular IT submissions being made.

13.7 A formal IT strategic planning process be implemented, including a procedure for the continual re-alignment of the IT objectives to those of the organisation.

13.8 The impact of IT impact on society and the environment be considered and how IT could promote sustainability.

13.9 An IT governance framework be established for the organisation, providing guidance on the process, structures and practices to be implemented to achieve effective IT governance.

13.10 An IT Steering Committee be established to oversee IT investment, priorities and resource allocation, on behalf of the Board.

13.11 The CIO should be the single point of accountability for IT to the Steering Committee.

13.12 An IT Strategy Committee be established or the combined responsibility for IT strategy and IT investment, priorities and resource allocation be made the combined responsibility of the IT Steering Committee, to involve the Board in strategic IT decisions.

13.13 The IT Steering Committee should monitor significant investments for value in terms of IT strategy and appropriateness of resource allocation to the investment. Compliance with the procurement policy should also be monitored.

13.14 An IT vendor management process be implemented.

13.15 At a minimum, a basic IT value management process be implemented. Where feasible, IT portfolio management be implemented to track the value derived from IT investments.

13.16 IT should submit regular reports to the IT Steering Committee to enable the Board to monitor the execution of the IT strategy and IT service delivery in general.

13.17 A risk assessment process be implemented that requires at least an annual, comprehensive IT risk assessment and regular updates to the IT risk understanding, all of which are documented and monitored in a formal IT risk register.

13.18 The agendas of all risk and audit committee meetings should provide for a section on IT-related risk and control reporting.

13.19 Business continuity management should not be regarded as an IT responsibility, but IT should be able to clearly demonstrate how its IT service continuity planning satisfies business continuity management requirements, as is expected of all departments in the organisation.

13.20 Formal information management practices be implemented to monitor the quality of data and information, compliance with privacy regulations and stakeholder requirements, and information security management.

13.21 An IT compliance framework be implemented to ensure that all IT stakeholders', legislative, regulatory, and corporate requirements are met.

**Participant comment**

### ISO/IEC38500 – Recommendation 14

14.1 An IT role player matrix should be implemented, showing all roles' responsibilities and accountabilities, as well as which roles need to be consulted or informed in the performance of IT duties.

14.2 Performance management should be implemented at staff, structure and process levels, to monitor how responsibilities are being fulfilled.

14.3 An IT PMO should be implemented if no EPMO exists to manage all projects, including those in IT. The PMO accepts responsibility for the implementation of IT projects.

14.4 The systems development lifecycle and project management methodology should be formalised as mechanisms for implementing strategy.

14.5 A process should be implemented for integrating IT strategic planning and the operation of the IT PMO, in order to translate IT strategy into execution.

14.6 An enterprise architecture function should be implemented to blueprint core aspects of the business and the manner in which IT should enable it.

14.7 IT Infrastructure management should be implemented, with renewal plans to ensure that the execution of IT strategy is sustained at an infrastructural level.

14.8 Strategic sourcing should be practiced as part of the IT vendor management process.

14.9 An IT assets lifecycle management process should be implemented to support IT planning and ensure the optimal use of IT assets.

14.10 Formal IT service support and service delivery processes should be implemented to ensure consistent, efficient IT services.

14.11 The key IT metrics should be defined, monitored and reported on an ongoing basis.

14.12 Formal processes should be implemented for IT planning, IT service management, project management, the systems development lifecycle, information security management, IT risk management, and EA.

14.13 Risk and control self assessment should be implemented as a mechanism to continually monitor compliance.

14.14 IT roles and responsibilities should be formalised, including the following:

14.14.1 Formal job descriptions should be implemented;

14.14.2 Incompatible duties should be segregated;

14.14.3 Performance management should be practiced in line with job descriptions;

14.14.4 Formal planning should be done for skills development and retention; and

14.14.5 Formal performance management should be implemented.

**Participant comment**

### IT Sub Processes – Recommendation 15

It is recommended that sub processes for the IT environment be formalised under each of the IT governance major processes in line with the desirable practices recommended in this paper. Each process should be supported by policies, procedures and standards setting out the mechanisms, structures and controls for effective operation of the process.

**Participant comment**

### IT Control Framework – Recommendation 16

As part of the proposed IT governance framework, it is recommended that IT controls be formalised in an IT control framework, based on the COBIT 4.1 control objectives and other relevant control objectives, e.g. those contained in ISO/IEC27000, for information security. The COBIT sub paragraph above has dealt with COBIT in detail.

**Participant comment**

### Supporting Documents – Recommendation 17

It is recommended that the policies, procedures and standards required to govern each key (high-priority) process be formalised, that a risk assessment be performed to highlight all high risk areas, and that an IT control framework be implemented to mitigate the identified risks. These documents should be reviewed and updated at least annually. The ultimate accountability for the effectiveness of policies, procedures and standards, and for the execution of risk assessments, resides with the CIO.

**Participant comment**

### Architecture – Recommendation 18

Enterprise architectrure (EA) is an important mechanism for integrating IT and the business. The proposed IT governance framework recommends that organisations should, at a minimum, embark upon an exercise to investigate an appropriate approach to enterprise architecture and to document their findings for consideration once the organisation has reached a level of maturity where a formal architecture function becomes feasible. The framework is not prescriptive about the roles within the EA function or what reporting lines should be followed.

**Participant comment**

### Portfolio Management – Recommendation 19

Recognising the developing nature of portfolio management, it is recommended that organisations should, (i) explore how portfolio management will be utilised in future IT investments and management; (ii) establish a mechanism to align IT spend (and related projects) to organisational objectives; (iii) take note of the development and maturing of the ValIT framework; and (iv) consider how the ITIL Service Portfolio Management process could benefit the organisation.

**Participant comment**

### Summarised Recommendation on Desirable Practices – Recommendation 20

To summarise the recommendations in this section, Table 1 maps the practices discussed in this paper to the IT governance major processes they are recommended to support.

| | CobiT | ITIL | PMBOK, Prince2 | ISO17799, ISO27001 | TOGAF | Balanced Scorecard | Portfolio Management | King III | ISO38500 |
|---|---|---|---|---|---|---|---|---|---|
| Strategic alignment | X | X | | | X | | X | X | X |
| Value delivery | X | X | X | | | | X | X | X |
| Risk management | X | X | | X | | | X | X | X |
| Resource management | X | X | X | | | | | X | X |
| Performance measurement | X | | | | | X | | X | X |

*Table 1 – Summary of Practices Supporting IT Governance Major Processes*

**Participant comment**

## IT Governance Structure Recommendations

### Office of the CIO – Recommendation 21

This paper does not insist on the existence of a CTO role. Rather, it is recommended that either the definition of the CIO role be broadly defined to incorporate the role of the CTO or the roles of the CTO and CIO be clearly segregated. The CIO role is rapidly changing and needs to be adjusted continually to keep up with new demands. Each organisation should define the CIO role to meet its strategic IT requirements. These requirements will determine the value IT should deliver and consequently the role of the individual leading the function.

**Participant comment**

### Chief Technology Officer – Recommendation 22

It is recommended that the creation of a CTO role should be based on a strategic decision and the nature of the organisation. Not all organisations are able to justify a CTO role. Organisations which have made a significantly higher investment in IT infrastructure than their peers, as well as telecommunications organisations, would probably find it easier to justify a CTO role.

**Participant comment**

### Information Security Officer (ISO) – Recommendation 23

The ISO role should be clearly defined and segregated from the implementation and administration of these policies, procedures and standards, as the most senior information security oversight function. If possible, it should be based outside IT.

**Participant comment**

### Chief Enterprise Architect – Recommendation 24

It is recommended that organisations' IT strategies make provision for the creation or maturing of the enterprise architecture role. Where feasible, this role should not be regarded as an IT function but rather be based closer to corporate strategy, with its technology-specific roles being resourced from IT.

**Participant comment**

### IT Financial Manager – Recommendation 25

It is recommended that the IT financial management role be formally assigned in all environments, but that the feasibility of creating a full-time position around it be carefully evaluated based on the size and complexity of the environment.

**Participant comment**

### IT Risk Officer – Recommendation 26

It is recommended that a formal IT risk officer role be created. Depending on the organisation it could then be decided whether to award this role as an additional responsibility to a senior IT official or to create a new position within IT for an operational risk manager. It is further imperative that all of the IT management team be made aware of their risk management responsibility.

**Participant comment**

### Applications Manager – Recommendation 27

It is recommended that, where feasible, the role of applications manager not be combined with other formal roles in large IT departments.

**Participant comment**

### Technical Manager – Recommendation 28

The proposed IT governance framework recommends that the technical management role be clearly defined and assigned to an individual who will then be responsible for all aspects of technical management. The framework does not dictate whether the technical manager or the applications manager owns and is responsible for the IT service support and IT service delivery processes, but requires these two roles to take responsibility for service support and service delivery between them.

**Participant comment**

### Operations Manager – Recommendation 29

It is recommended that each organisation evaluate whether or not the size of its IT department justifies the appointment of an operations manager. If not, this role could be combined with that of the technical manager. This paper does not argue for any particular IT operations structure but recommends, (i) clear roles and responsibilities for each operational area, and (ii) a clear definition of the operations management role.

**Participant comment**

### IT Strategy Committee – Recommendation 30

It is recommended that all organisations have an IT Strategy Committee comprising top executives and the CIO. In some organisations, this committee would also be responsible for areas assigned to the IT Steering Committee below.

**Participant comment**

### IT Steering Committee – Recommendation 31

It is recommended that each organisation should have at least one IT governance body responsible for setting IT strategy (IT Strategy Committee) and one for overseeing the establishment of mechanisms for delivering the strategy (IT Steering Committee). Where feasible, these should be two different bodies but, provided the body does not involve itself in the actual implementation of strategy, the two could be one. Where the two bodies are segregated, the IT Strategy Committee membership should be as senior as possible, preferably Board level.

**Participant comment**

### Enterprise Architecture Forum – Recommendation 32

It is recommended that some kind of governance body be set up to oversee the establishment and effectiveness of EA in the organisation. Where possible, this function should be situated outside IT, as a corporate strategy implementation enabler.

**Participant comment**

### Programme Management Office (PMO) – Recommendation 33

Without being prescriptive as to where the IT PMO should reside, it is recommended that PMO principles be adopted to govern any significant IT projects. It is further recommended that a formal, standardised project management methodology be adopted, including a project management maturity model, whether for IT or at an enterprise level. The adopted project management methodology should contain a project management maturity model, indicating maturity targets for project management.

**Participant comment**

### Summarised Recommendation on IT Governance Roles – Recommendation 34

To summarise the recommendations on IT management roles in this section, Table 2 maps the roles discussed in this paper to the IT governance major processes they are recommended to support.

| | CIO | CTO | ISO | Applications Manager | Enterprise Architect | Technical Manager | Operations Manager | IT Financial Manager | IT Risk Officer |
|---|---|---|---|---|---|---|---|---|---|
| Strategic alignment | A | R | I | C | R | C | I | C | R |
| Value delivery | A | C | C | R | C | R | R | R | C |
| Risk management | A | R | R | R | R | R | R | R | R |
| Resource management | A | R | C | R | I | R | R | R | C |
| Performance measurement | A | R | R | R | C | R | R | R | R |

*Table 2 –IT Management Roles per IT Governance Major Process*

**Participant comment**

### Summarised Recommendation on IT Governance Structures - Recommendation 35

To summarise the recommendations on structures in this section, Table 3 maps the structures discussed in this paper to the IT governance major processes they are recommended to support.

| | Office of the CIO | IT Steerig Committee | IT Strategy Committee | Enterprise Architecture Forum | Pogramme Management Office |
|---|---|---|---|---|---|
| Strategic alignment | R | C | A | R | R |
| Value delivery | R | A | C | C | R |
| Risk management | A | I | I | C | R |
| Resource management | A | C | I | C | R |
| Performance measurement | A | I | I | C | R |

*Table 3 – RACI Mapping for IT Governance Structures*

**Participant comment**

## APPENDIX B – STRUCTURED INPUT SCHEDULE

| | | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all |
|---|---|---|---|---|---|---|
| | **A. GENERAL** | | | | | |
| a | How important is the Office of the CIO concept to you? | □ | □ | □ | □ | □ |
| | | □ | □ | □ | □ | □ |
| b | How important is the inclusion of operational roles below that of CIO in the framework? | □ | □ | □ | □ | □ |
| b.1 | Please elaborate on your response to b above, i.e. why do you see value in the inclusion of these rules or why do you believe they should be excluded? | □ | □ | □ | □ | □ |
| | They are responsible for execution and demand management | | | | | |
| | | | | | | |
| c | How important is the role of an IT financial manager? | □ | □ | □ | □ | □ |
| c.1 | Should the IT financial manager role be permanent or merely an allocated responsibility? Please tick one option. | | | | | |
| c.1.1 | Permanent | | | | | □ |
| c.1.2 | Allocated | | | | | □ |
| | | | | | | |
| d | How important is the role of an IT risk officer? | □ | □ | □ | □ | □ |
| d.1 | Should the IT risk officer role be permanent or merely an allocated responsibility? | | | | | |
| d.1.1 | Permanent | | | | | □ |
| d.1.2 | Allocated | | | | | □ |
| | | | | | | |
| | How important is the role of the: | | | | | |
| e | Applications manager? | □ | □ | □ | □ | □ |
| f | Technical manager? | □ | □ | □ | □ | □ |
| g | IT operations manager? | □ | □ | □ | □ | □ |
| | | | | | | |
| h | How important is it to segregate IT operations and technical manager roles? | □ | □ | □ | □ | □ |
| | | | | | | |
| i | Who should be responsible for IT service support? Please tick one | | | | | |

| | | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all |
|---|---|---|---|---|---|---|
| i.1 | Applications manager | | | | | |
| i.2 | Technical manager | | | | | |
| i.3 | Operations manager | | | | | |
| i.4 | A dedicated IT service support manager reporting to the technical manager role | | | | | |
| i.5 | A dedicated IT service support manager reporting to the operations manager | | | | | |
| | | | | | | |
| j | Who should be responsible for IT service delivery? Please tick one | | | | | |
| j.1 | Applications manager | | | | | |
| j.2 | Technical manager | | | | | |
| j.3 | Operations manager | | | | | |
| j.4 | A dedicated IT service delivery manager reporting to the technical manager role | | | | | |
| j.5 | A dedicated IT service delivery manager reporting to the operations manager role | | | | | |
| | | | | | | |
| k | Do you believe an IT governance framework should be prescriptive on whether a centralised, federated or hybrid IT organisational model should be adopted? Please tick “yes” or “no” | | | | | |
| k.1 | Yes | | | | | |
| k.1.1 | If, “yes”, please elaborate on your thinking | | | | | |
| | The specific model select will influence the control framework | | | | | |
| k.2 | No | | | | | |
| l | How important is vendor management to an IT governance framework? | | | | | |
| | | | | | | |
| m | Which of the following options do you prefer for IT procurement? Please tick one | | | | | |
| m.1 | IT procurement should be a normal part of the corporate procurement process | | | | | |
| m.2 | IT procurement should be a process independent of the corporate procurement process | | | | | |
| | | | | | | |
| n | Which of the following options do you prefer (please tick one) for IT vendor management? | | | | | |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all |
|---|---|---|---|---|---|---|
| n.1 | IT procurement should be a normal part of the corporate procurement process but IT vendor management should be separate from the corporate function |  |  |  |  |  |
| n.2 | IT procurement and IT vendor management should be separate from the corporate function and procurement processes |  |  |  |  |  |
|  |  |  |  |  |  |  |
| o | How important is the role of an IT Steering Committee in your organisation? |  |  |  |  |  |
| p | How important is the role of an IT Strategy Committee in your organisation? |  |  |  |  |  |
|  |  |  |  |  |  |  |
| q | Would you prefer to have separate IT Strategy and Steering Committees or combine them?  Please tick one option. |  |  |  |  |  |
| q.1 | Separate |  |  |  |  |  |
| q.2 | Combined |  |  |  |  |  |
|  |  |  |  |  |  |  |
| r | How important is it to have a formal chief technology officer role? |  |  |  |  |  |
| s | How important is it to segregate the chief technology officer role from that of the CIO and other IT roles? |  |  |  |  |  |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
|  | ***Practices*** |  |  |  |  |  |
| t | How important is implementing the IT governance chapter of the King III Code of Corporate Governance to your IT governance objectives? |  |  |  |  |  |
| u | How important is implementing the concepts of the ISO/IEC38500 IT governance standard to your IT governance objectives? |  |  |  |  |  |

|  |  |  |
|---|---|---|
|  | **B.  STRATEGIC ALIGNMENT** |  |
|  | ***IT Goals and Objectives*** |  |
|  | How often **<u>should you</u>** revisit your IT strategy and re-align it to the corporate strategy?  Please tick one |  |
| a | Annually |  |
| b | Annually, with an update halfway through the year |  |
| c | Every third year |  |
| d | Every third year, with annual updates |  |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all |
|---|---|---|---|---|---|---|
| e | A different frequency from the above – please specify |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  | ***Enterprise Architecture*** |  |  |  |  |  |
|  | Which of the following statements do you agree with?  Please tick each option you agree with |  |  |  |  |  |
| f | Enterprise architecture is a business rather than IT function |  |  |  |  |  |
| g | The business architecture belongs to business, the remaining architecture layers belong to the IT function |  |  |  |  |  |
| h | Enterprise architecture should be closely linked to the corporate strategy function, to translate strategy to action |  |  |  |  |  |
| i | How important is the role of a dedicated enterprise architect in your organisation? |  |  |  |  |  |
| j | How important is the role of an enterprise architecture forum to your organisation? |  |  |  |  |  |
| k | It is important to align IT services to the IT strategy on an ongoing basis |  |  |  |  |  |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
|  | ***Practices*** |  |  |  |  |  |
|  | How important is each of the following to practising sound IT governance? |  |  |  |  |  |
| l | Following TOGAF as a desirable practice |  |  |  |  |  |
| m | Following an enterprise architecture methodology, regardless of the adopted practice |  |  |  |  |  |
| n | Integration between enterprise architecture and corporate strategy |  |  |  |  |  |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
|  | **C.  VALUE DELIVERY** |  |  |  |  |  |
|  | How important is each of the following to sound value delivery in your organisation? |  |  |  |  |  |
| a | Having an enterprise PMO that also handles IT projects |  |  |  |  |  |
| b | Having an IT PMO, regardless of whether an enterprise PMO exists or not |  |  |  |  |  |
| c | Including IT portfolio management in enterprise portfolio management |  |  |  |  |  |
| d | Practising IT portfolio management, regardless of whether enterprise portfolio management is practised or not |  |  |  |  |  |
| e | Practising IT service portfolio management to ensure continual alignment of services to the organisational strategy |  |  |  |  |  |
| f | Following the development of ValIT and implementing the framework once it has matured sufficiently |  |  |  |  |  |
| g | Following a formal project management methdology |  |  |  |  |  |
| h | Practising formal service level management |  |  |  |  |  |

| | | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all |
|---|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| | ***Practices*** | | | | | |
| | How important is each of the following to practising sound IT governance in your organisation? | | | | | |
| i | Following Prince2 as a project management method | | | | | |
| j | Following PMBOK as the underlying project management philosophy, regardless of what other methodologies are used | | | | | |
| k | Having any formal project management methodology, regardless of whether it is Prince2 or another | | | | | |
| l | Monitoring the development of ValIT as a value mangement practice, in order to consider its adoption once it has matured sufficiently | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **D. RESOURCE MANAGEMENT** | | | | | |
| | How important is each of the following to sound IT resource management in your organisation? | | | | | |
| a | Adhering to corporate resource management processes, as part of practising IT governance | | | | | |
| b | Implementing formal IT service support and service delivery processes | | | | | |
| c | Implementing a dedicated help desk or service desk to facilitate effective IT service management | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | ***Practices*** | | | | | |
| | How important is each of the following to practising sound IT governance in your organisation? | | | | | |
| d | Using ITIL as the underlying practice for structuring IT services, support and delivery | | | | | |
| e | Implementing formal software asset management to manage the software lifecycle | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **E. RISK MANAGEMENT** | | | | | |
| | How important is each of the following to sound IT risk management in your organisation? | | | | | |
| a | Integrating IT risk management with the operational risk management component of enterprise risk management (ERM) | | | | | |
| b | Maintaining an IT risk management function in IT, rather than having it as part of ERM | | | | | |
| c | Having formally identified, categorised and classified information assets | | | | | |
| d | Performing annual IT risk assessments, with six-monthly follow up | | | | | |
| e | Having a formal information security management function in IT | | | | | |
| f | Having a formal information security management function that is segregated from IT, i.e. as a business function | | | | | |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all |
|---|---|---|---|---|---|---|
| g | Having a formally assigned IT security officer role, allocated to a person in IT |  |  |  |  |  |
| h | Having a formally assigned IT security officer role, allocated to a person outside IT |  |  |  |  |  |
| i | Having a full-time information security officer |  |  |  |  |  |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
|  | ***Practices*** |  |  |  |  |  |
|  | How important is each of the following to practising sound IT governance in your organisation? |  |  |  |  |  |
| j | Using ISO/IEC27000 as the basis for managing information security |  |  |  |  |  |
| k | Basing the IT control environment on COBIT |  |  |  |  |  |
| l | Formalising IT processes, policies, procedures and standards |  |  |  |  |  |
| m | Implementing a formal IT control framework |  |  |  |  |  |
| n | Monitoring the development of Risk IT as a risk management practice, in order to consider its adoption once it has matured sufficiently |  |  |  |  |  |

|  |  |  |
|---|---|---|
|  | **F.  PERFORMANCE MEASUREMENT** |  |
|  | ***Performance Measurement Mechanism*** |  |
|  | Which of the following statements do you agree with?  Please tick one |  |
| a | It is important to implement an IT balanced scorecard |  |
| b | It is important to implement any performance management practice, whether in the form of a balanced scorecard or not |  |

|  |  |
|---|---|
|  | **G.  CONCLUSION** |
| a | Are there other desirable IT governance practices not mentioned above that would be required by your organisation?  If so, please list them: |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| b | Are there other IT governance structures or roles not mentioned above that would be required by your organisation?  If so, please list them: |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| c | Are there other IT governance mechanisms not mentioned above that would be required by your organisation?  If so, please list them: | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| d | What do you consider to be the key requirements for sustainability in the IT context?  Please explain | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

# Appendix Two – Graphs Supporting Analysis

## A. General

### Question A-A

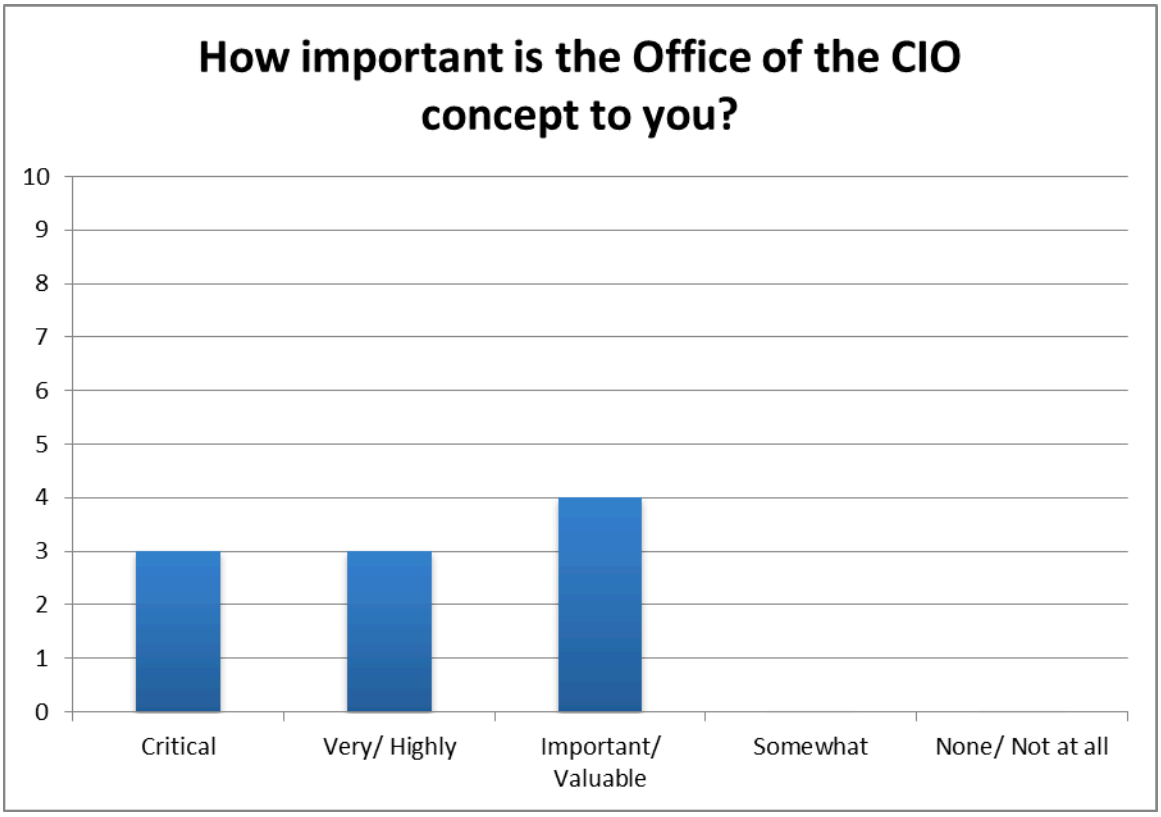


**Diagram a – Response to question A-A**

Question: How important is the Office of the CIO concept to you?

Classification: Accepted

Deduction: Most respondents agreed that the concept is highly important or critical to effective IT governance. All respondents agreed that there is value in the concept of the Office of the CIO. The four responses that fell into the *important/valuable* category were evenly distributed between public and private sector respondents.

Cross-reference: Recommendation 21

### Question A-B

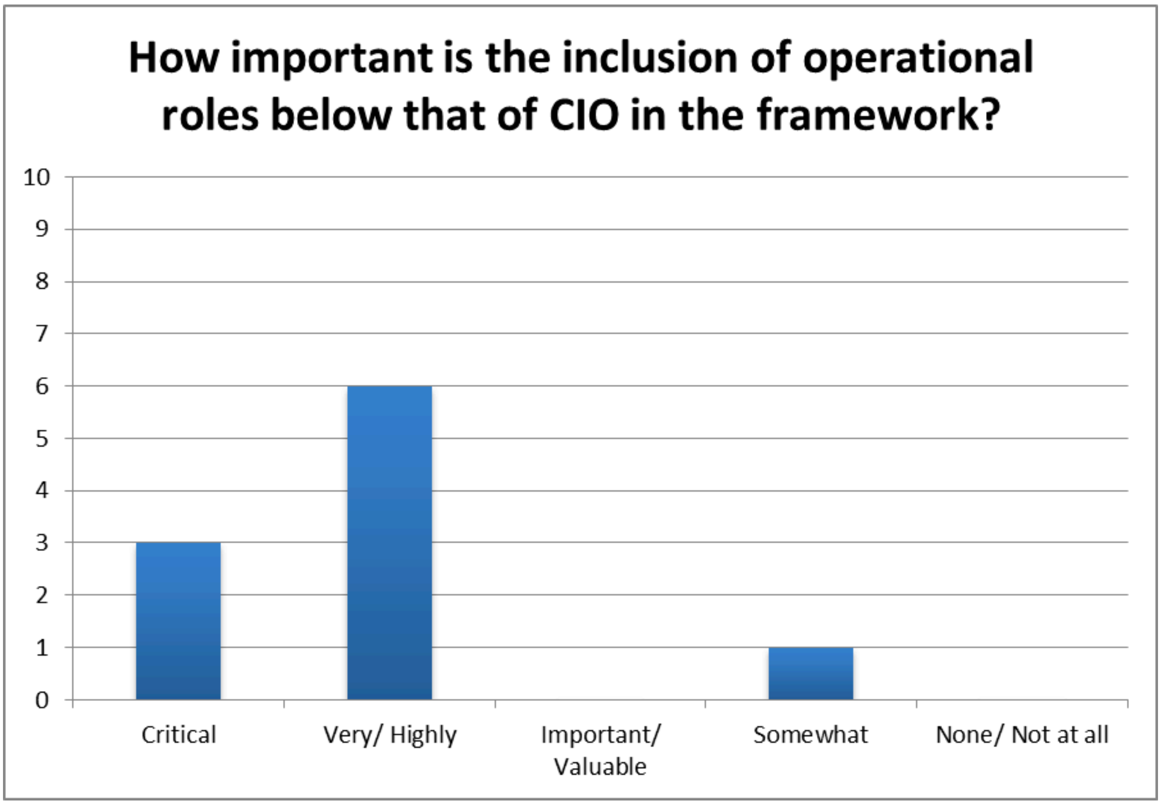


**Diagram b – Response to question A-B**

Question: How important is the inclusion of operational roles below that of CIO in the framework?

Classification: Accepted

Deduction: The effectiveness of the Office of the CIO depends on the clarity of roles making up the Office. One respondent did not see much value in the inclusion of IT operational roles in the IT governance framework.

Cross-reference: Recommendations 20-29

### Question A-C

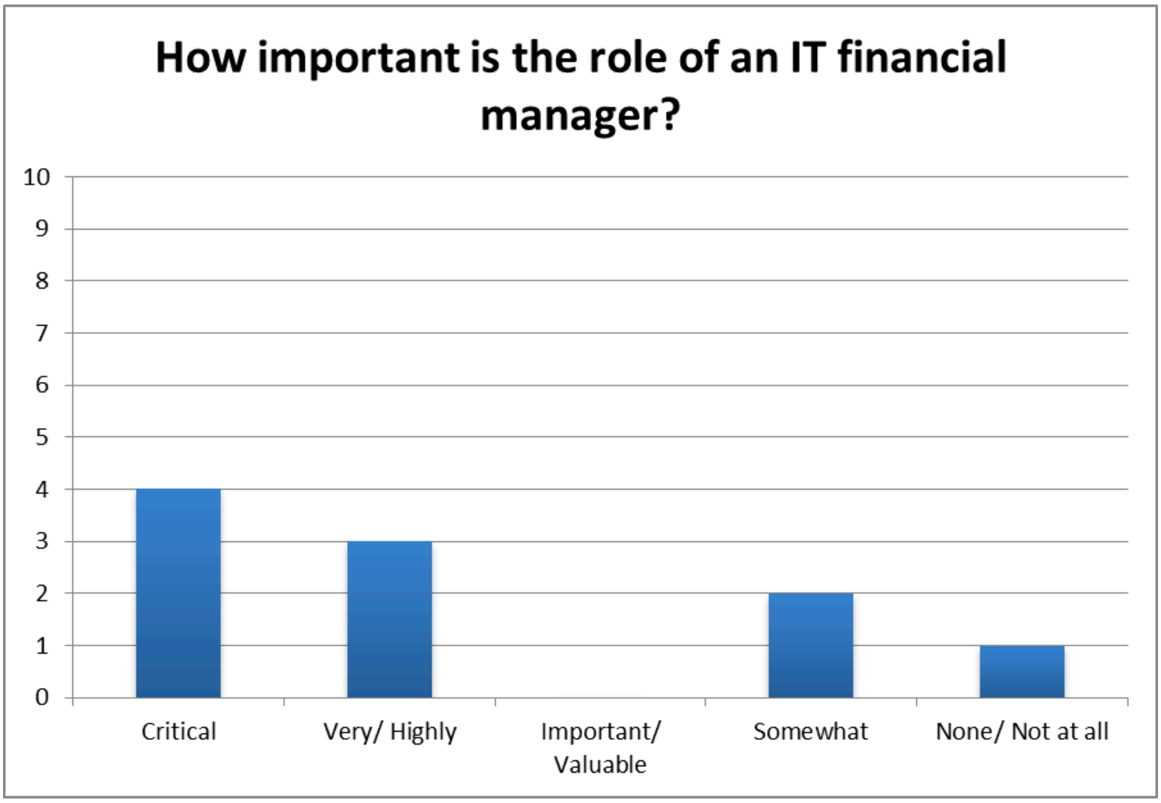


**Diagram c – Response to question A-C**

Question: How important is the role of an IT financial manager?

Classification: Accepted

Deduction: The IT financial manager role is of significant importance. Three of the public sector respondents did not see much value in the role, however, the majority of respondents regarded the role as highly or critically important, which indicates that IT financial management is more of a priority to the private sector.

Cross-reference: Recommendation 25

### Question A-C.1

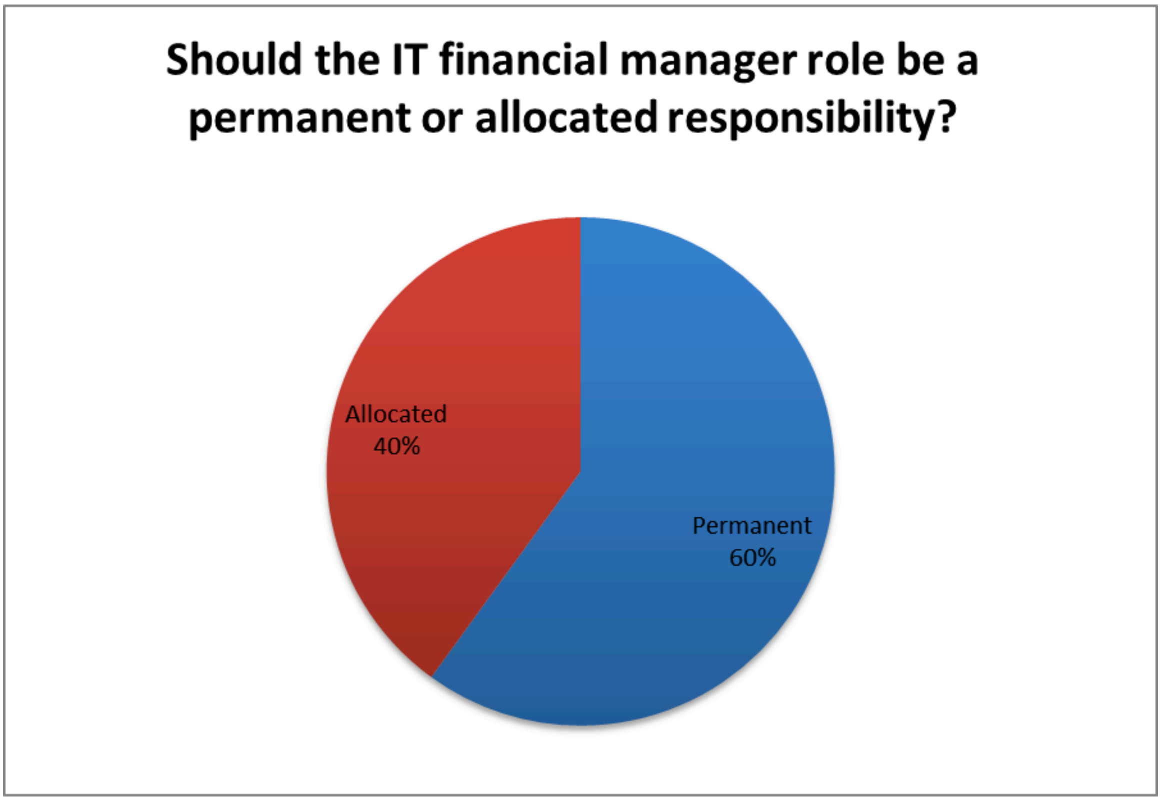


**Diagram d – Response to question A-C.1**

Question: Should the IT financial manager role be permanent or merely an allocated responsibility?

Classification: Accepted

Deduction: The IT financial manager role is important enough to warrant a full-time appointment. The same three public sector respondents who indicated that the role does not have much value replied consistently that the role should not be allocated full-time. In addition, one private sector respondent indicated that this should be a part-time role.

Cross-reference: Recommendation 25

### Question A-D

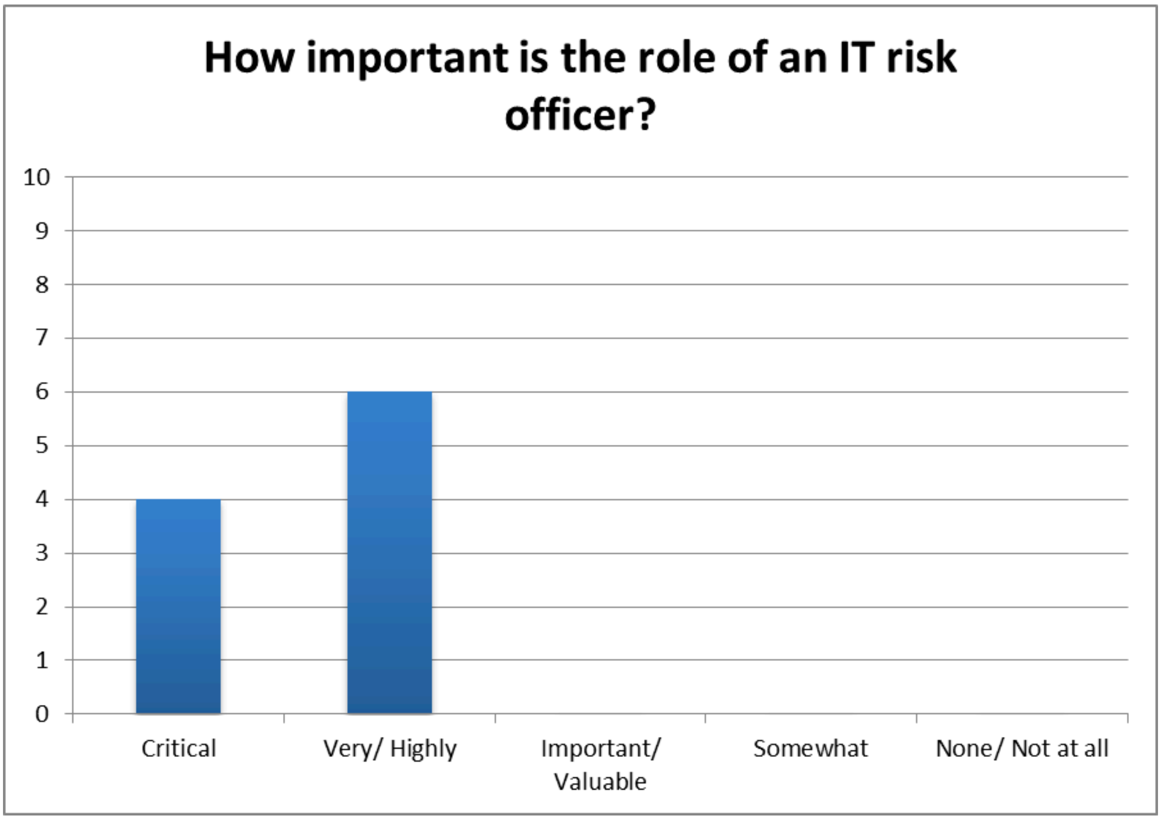


**Diagram e – Response to question A-D**

Question: How important is the role of an IT risk officer?

Classification: Accepted

Deduction: The IT risk officer role is of significant importance and warrants a full-time appointment. In the non-structured feedback, some of the participants felt that a broader role is required, in the form of an IT governance officer role. The researcher's interpretation is therefore that the role of an IT governance officer is of significant importance.

Cross-reference: Recommendation 26

*Question A-D.1*

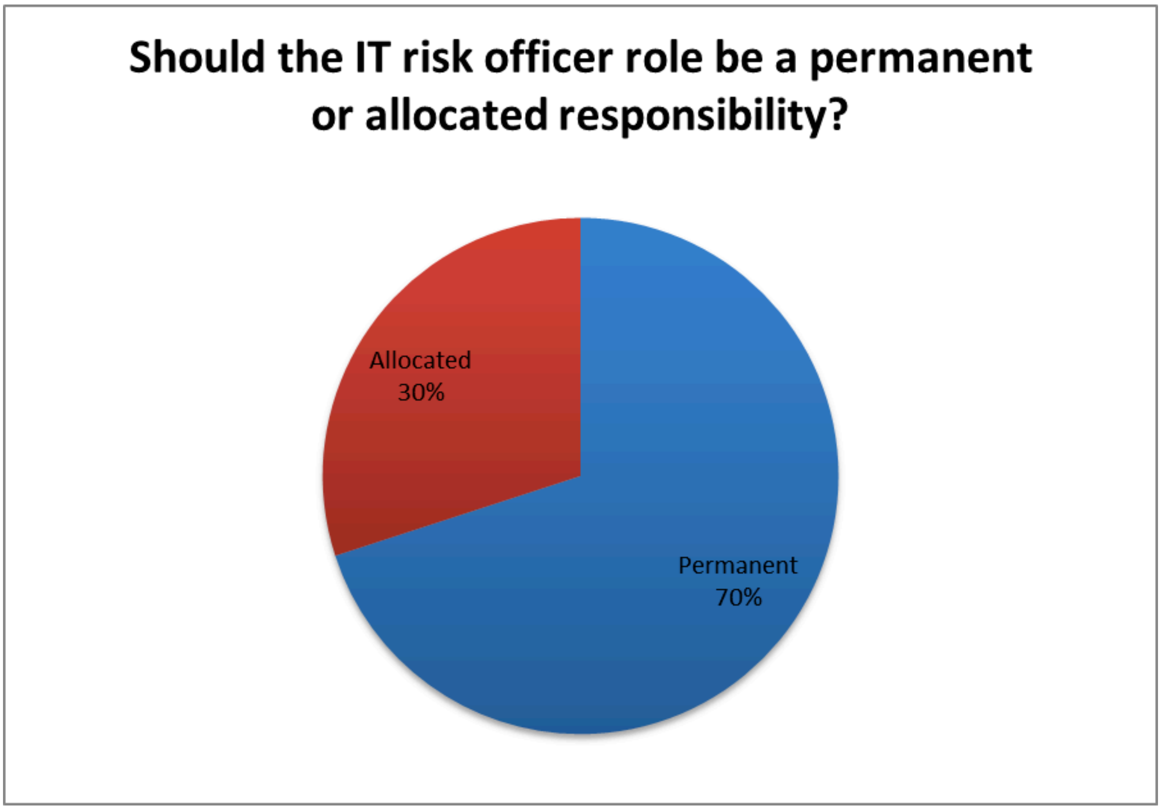


**Diagram f – Response to question A-D.1**

Question: Should the IT risk officer role be permanent or merely an allocated responsibility?

Classification: Accepted A-D.1.1 – The IT risk officer role should be a permanent responsibility.

Deduction: The IT risk officer role is of significant importance and warrants a full-time appointment. In line with the preceding question, this is interpreted as a requirement for a permanent IT governance officer role.

Cross-reference: Recommendation 26

### Question A-E

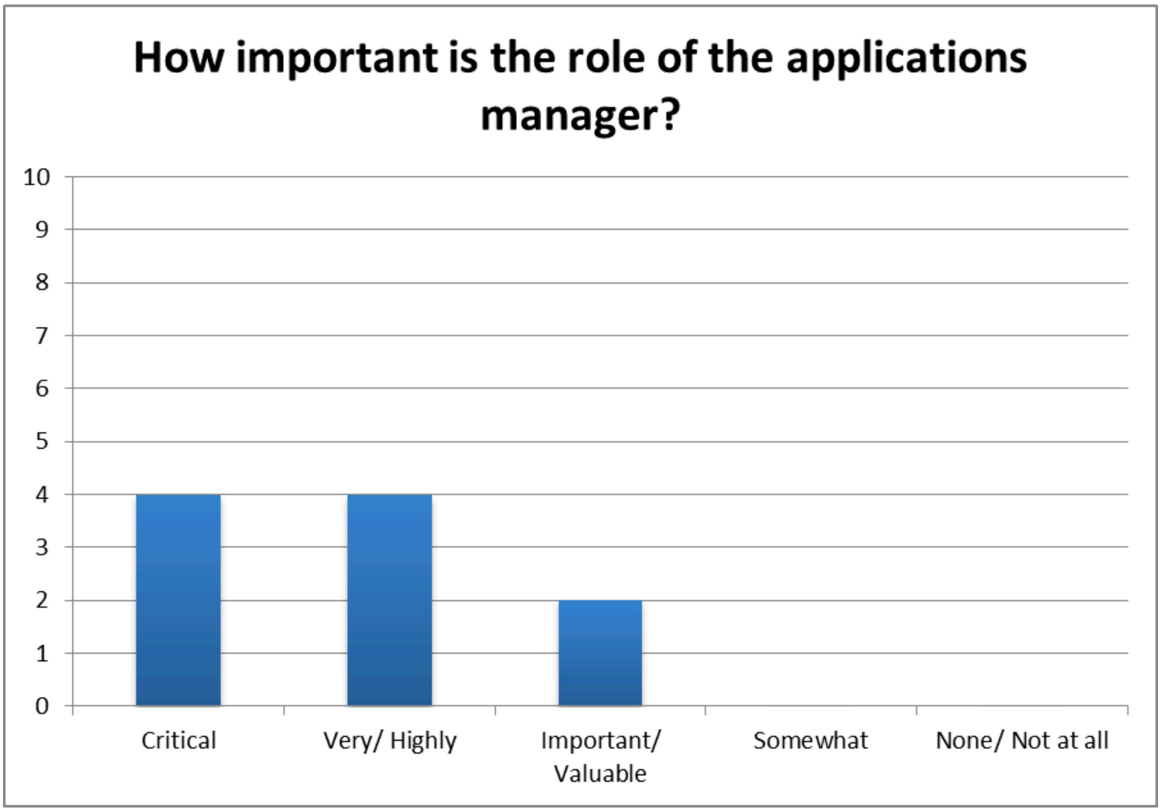


**Diagram g – Response to question A-E**

Question: How important is the role of the applications manager?

Classification: Accepted

Deduction: The role is of significant importance. In the instructured comment, participants indicated that the framework should elaborate on this role.

Cross-reference: Recommendation 27

## Question A-F

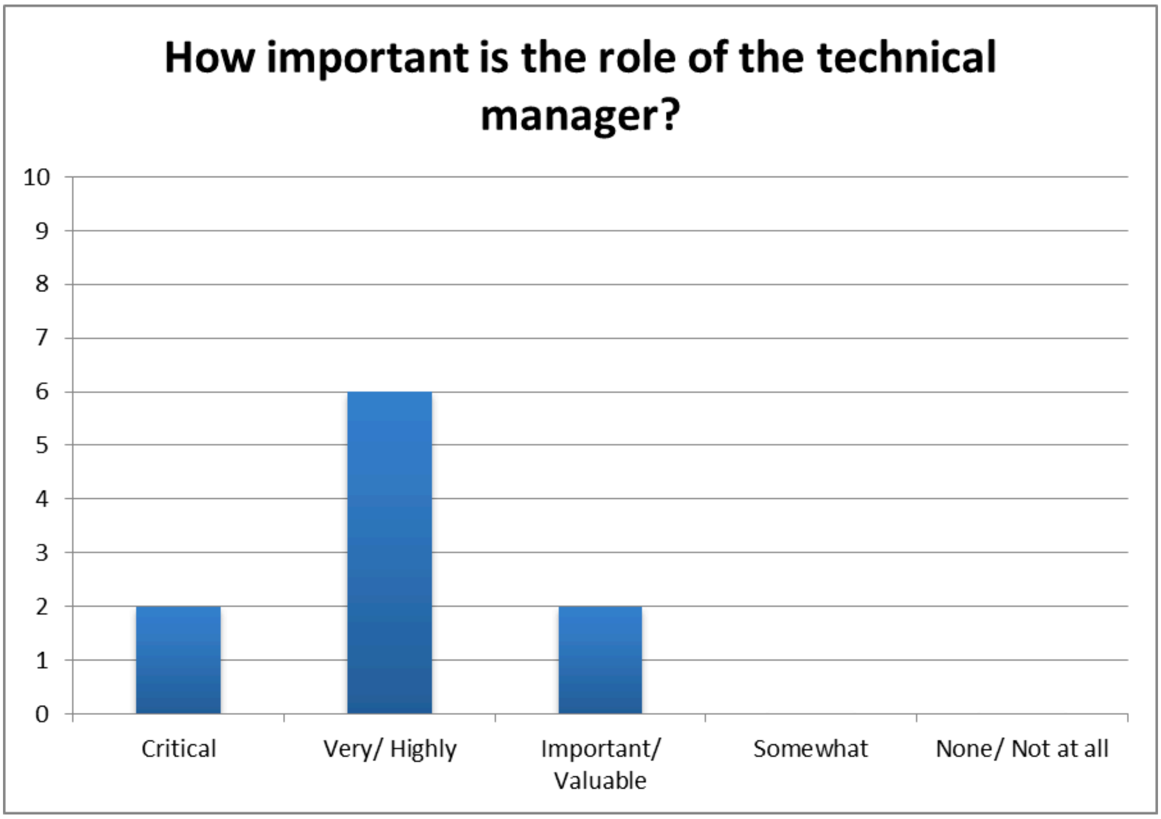


**Diagram h – Response to question A-F**

Question: How important is the role of the technical manager?

Classification: Accepted

Deduction: The role is of significant importance.

Cross-reference: Recommendation 28

### Question A-G

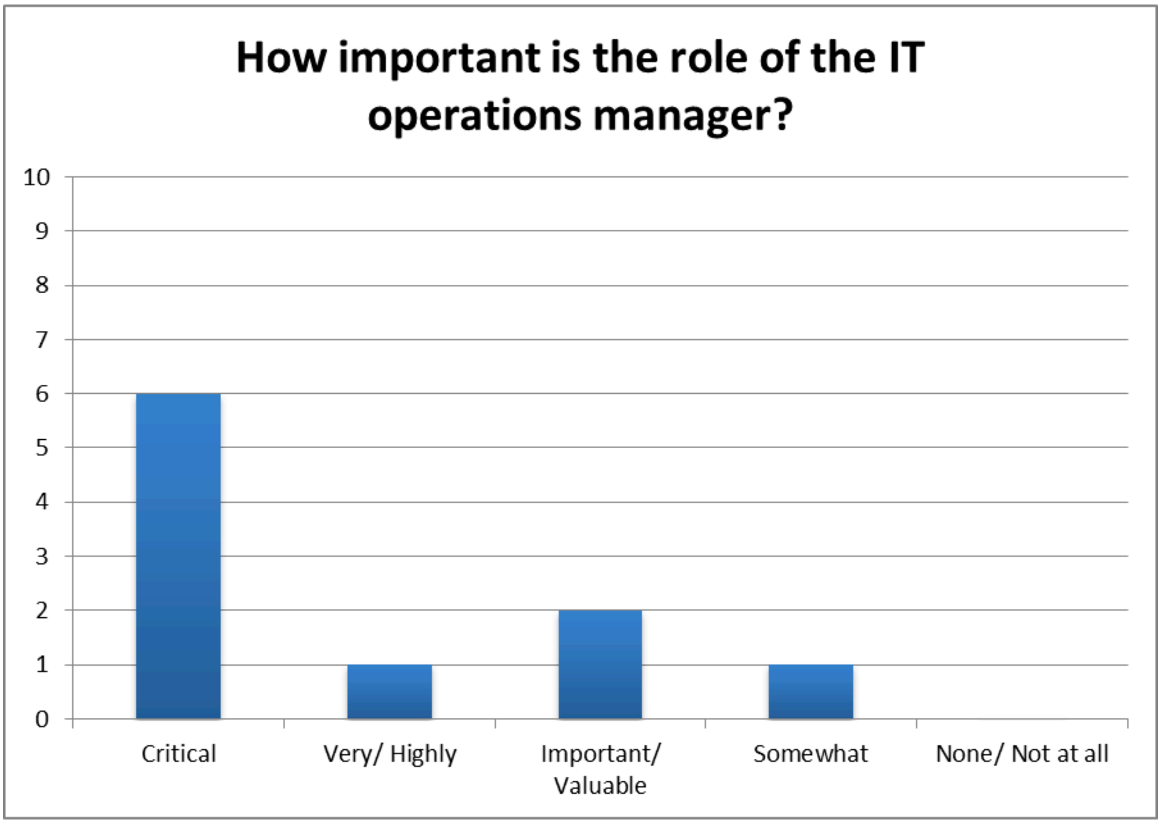


**Diagram i – Response to question A-G**

Question: How important is the role of the IT operations manager?

Classification: Accepted

Deduction: The role is of significant importance. Recommendation 29, which is supported by this question, was unanimously accepted.

Cross-reference: Recommendation 29

### Question A-H

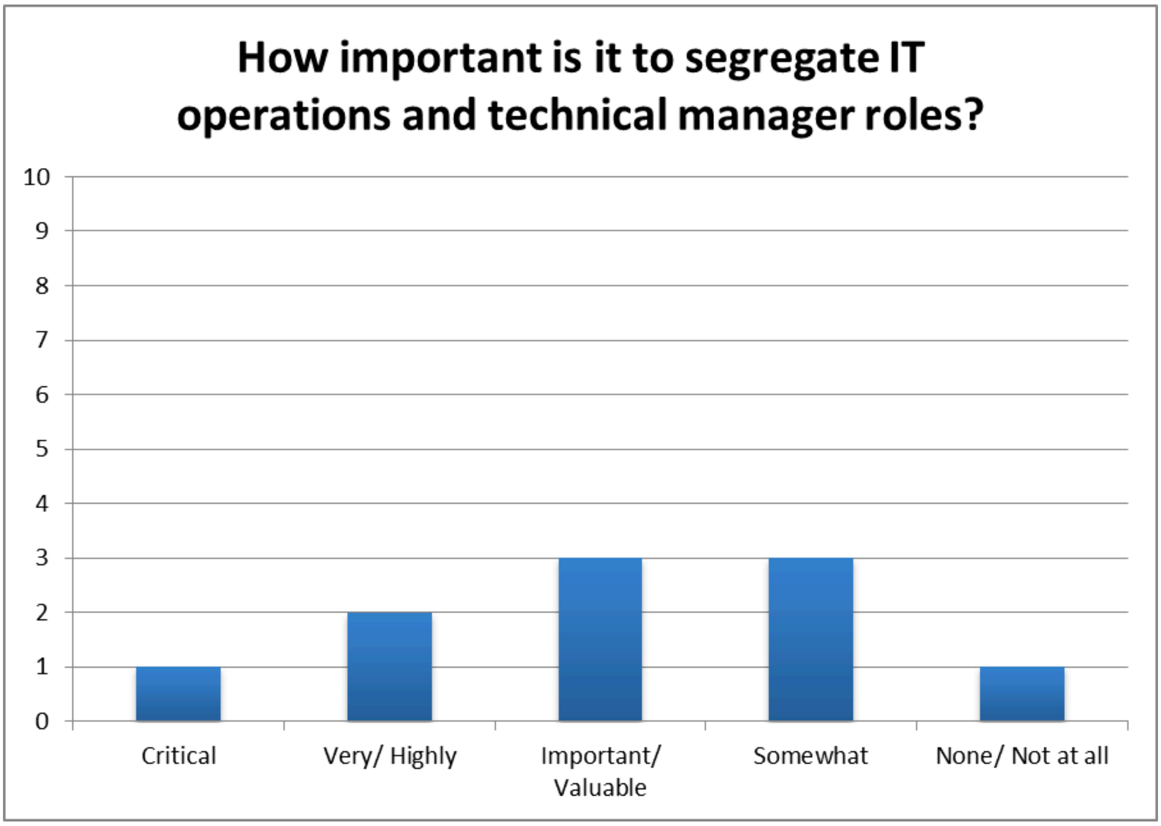


**Diagram j – Response to question A-H**

Question: How important is it to segregate IT operations and technical manager roles?

Classification: Considered

Deduction: The technical manager role could be combined with other roles without compromising its effectiveness.

Cross-reference: Recommendation 28

### Question A-I

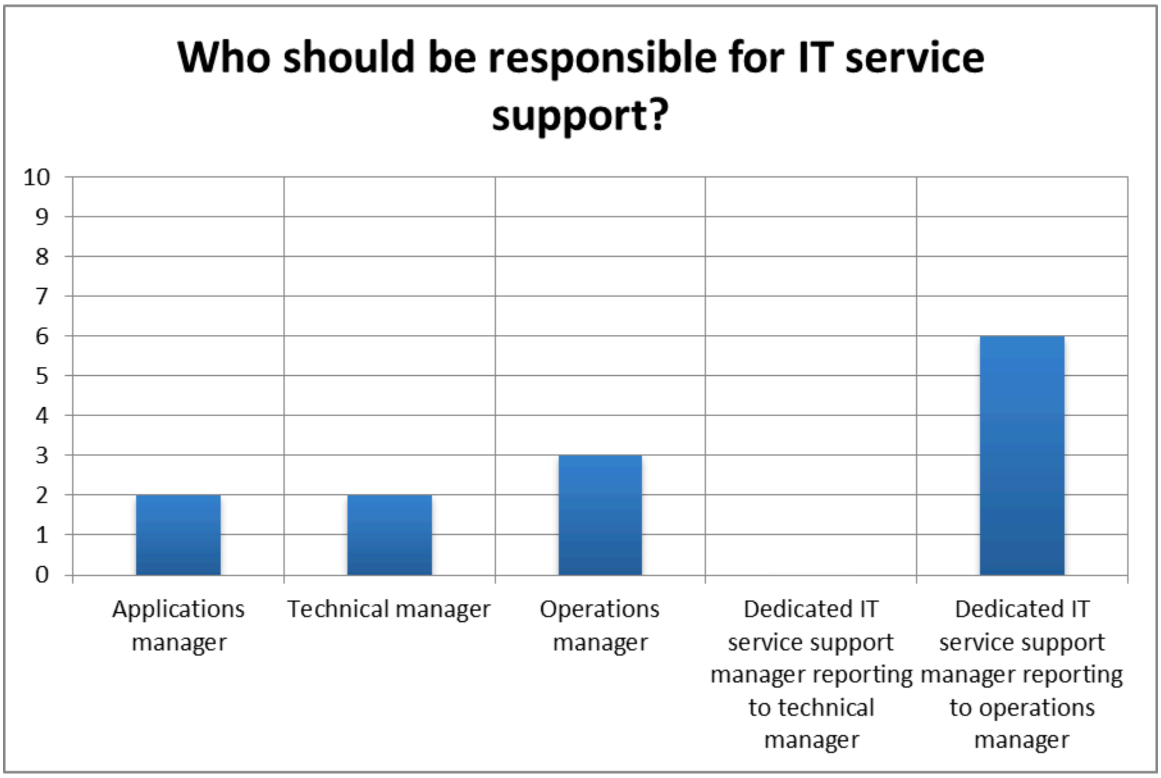


**Diagram k – Response to question A-I**

Question: Who should be responsible for IT service support?

Classification:

Applications manager: Not accepted

Technical manager: Not accepted

Operations manager: Not accepted

Dedicated IT service support manager reporting to technical manager: Not accepted

Dedicated IT service support manager reporting to technical manager: Accepted

Deduction: A dedicated service support role is significantly important, with a preferred reporting line to the operations manager. Three private sector respondents could not decide on a single role and indicated two choices. Two of these respondents came up with the same combination, namely the operations manager or an IT service support manager reporting to the operations manager, which is a practice more commonly found in large corporates, such as the organisations they represent. As a generic practice, though, it makes sense to create a dedicated IT service support role reporting to the operations manager.

Cross-reference: 28

### Question A-J

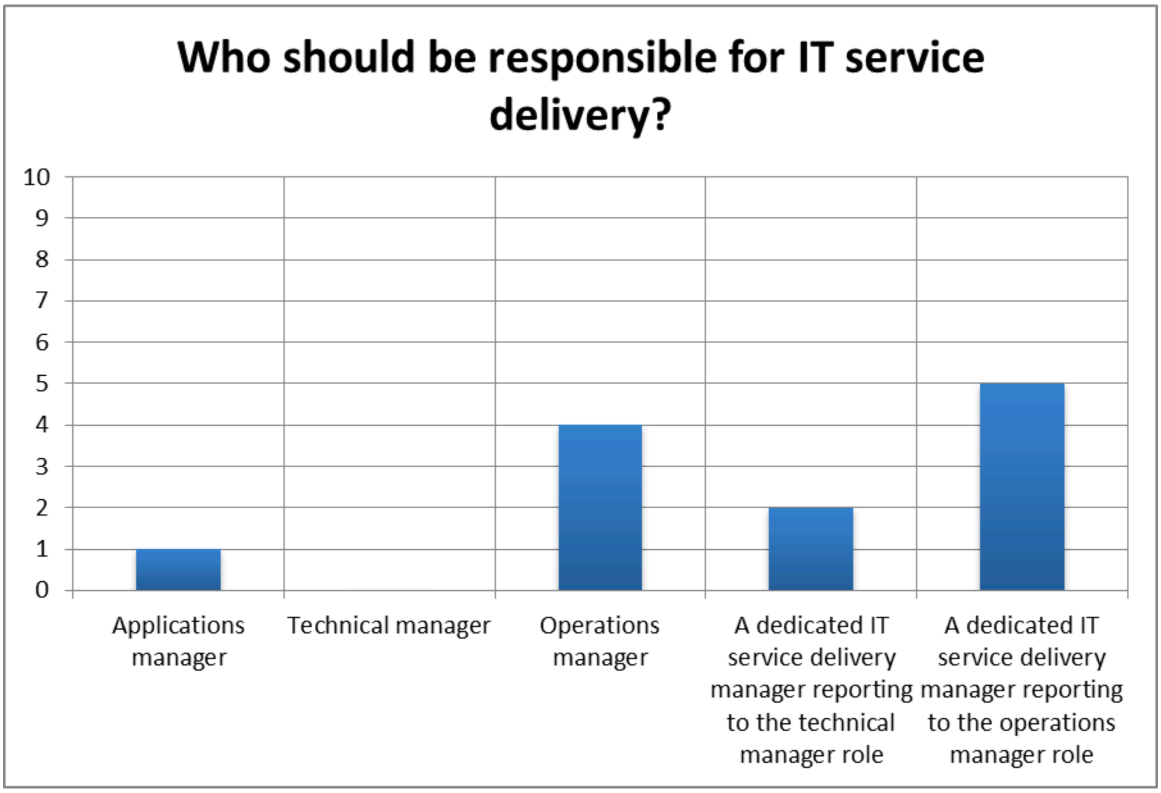


**Diagram I – Response to question A-J**

Question: Who should be responsible for IT service delivery? Please tick one.

Classification: Only accepted J.5 – A dedicated service delivery manager reporting to the operations manager role. Did not accept any of the other four options. Two participants selected both the third and fifth option.

Deduction: A dedicated IT service delivery role is significantly important, with a higher preference for this role reporting into the operations manager role than into the technical manager role.

Cross-reference: Recommendation 29

### Question A-K

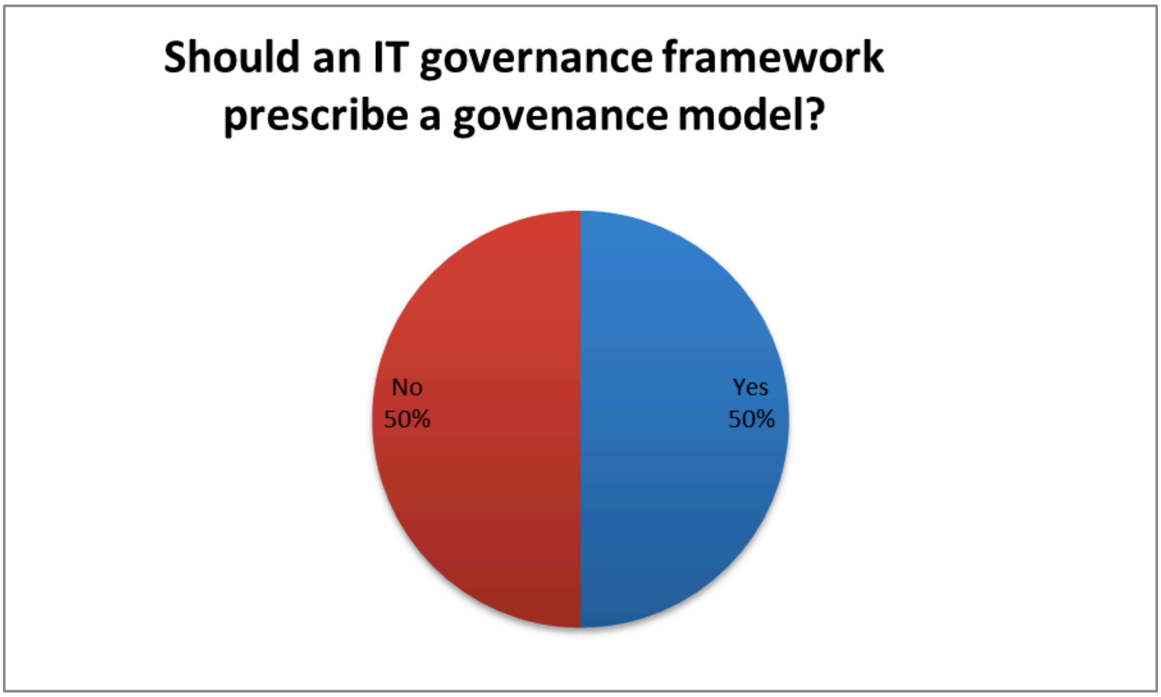


**Diagram m – Response to question A-K**

Question: Do you believe an IT governance framework should be prescriptive on whether a centralised, federated or hybrid IT organisational model should be adopted? Please tick “yes” or “no”.

Classification: Undecided

Deduction: The IT operational model depends on, and should follow, the culture of the organisation. This is the conclusion, based on the divided opinion to this criterion.

Cross-reference: Non-specific

### Question A-L

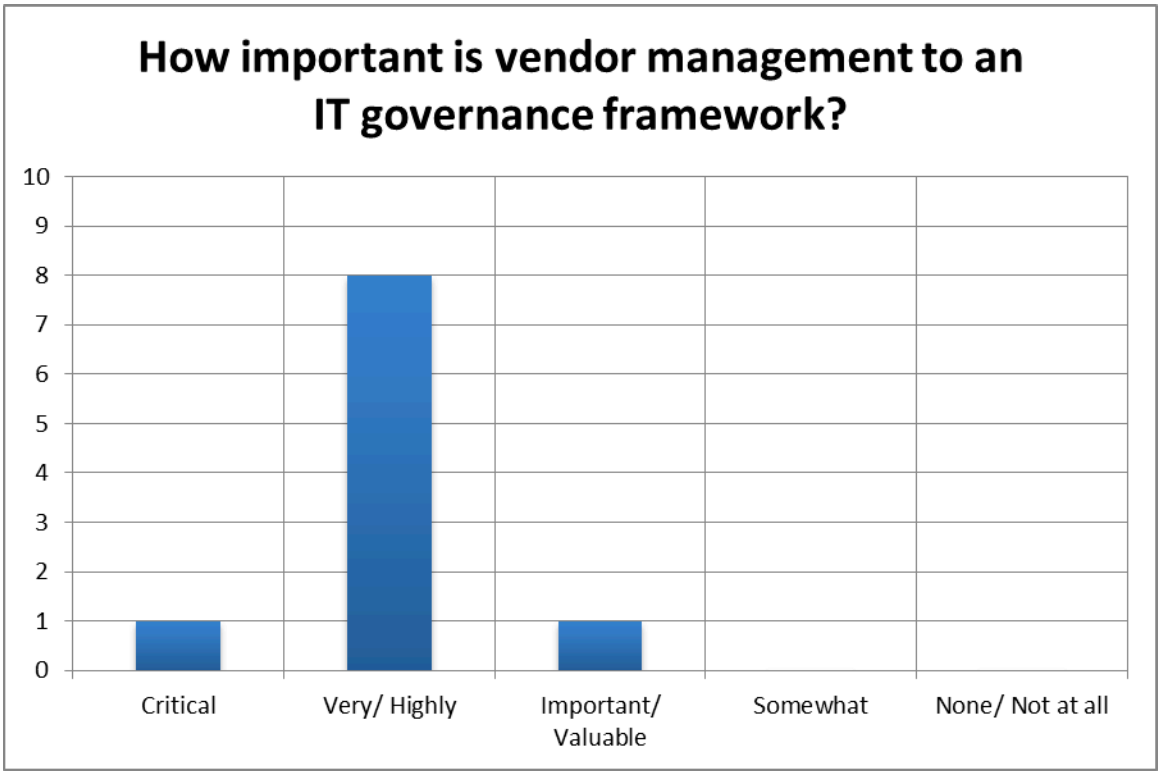


**Diagram n – Response to question A-L**

Question: How important is vendor management to an IT governance framework?

Classification: Accepted

Deduction: Vendor management is significantly important to the framework.

Cross-reference: Recommendations 3, 21

### Question A-M

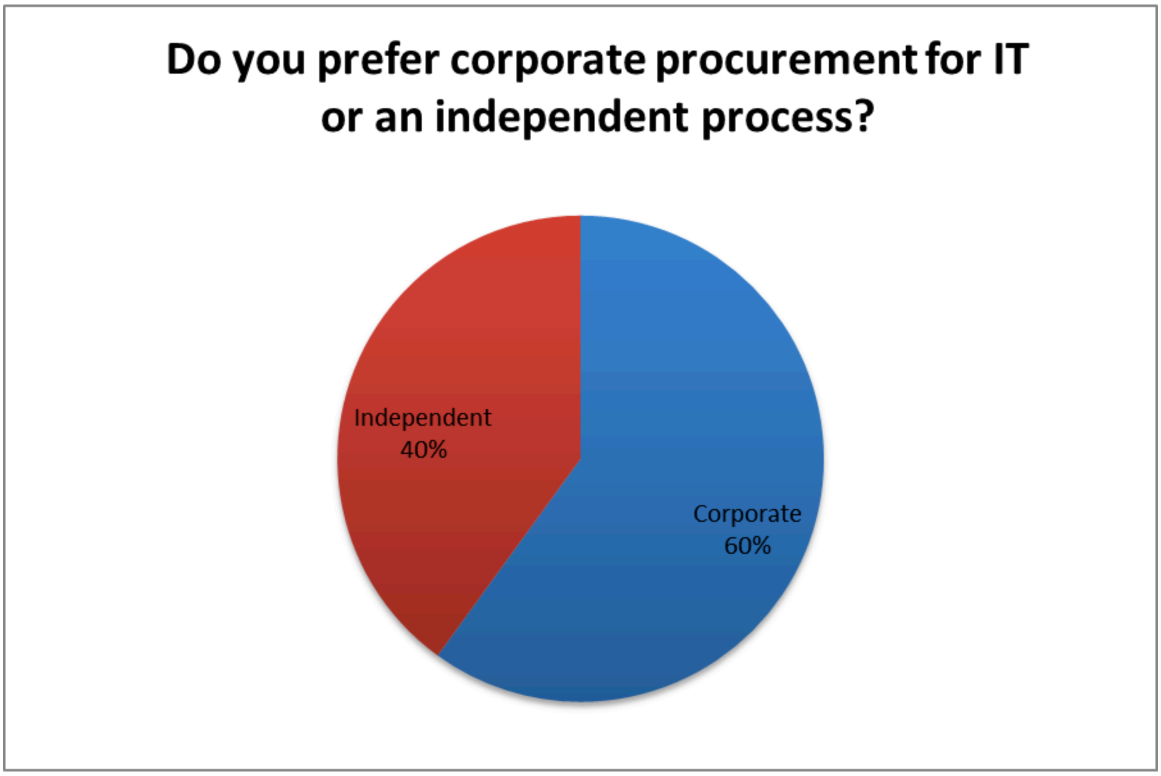


**Diagram o – Response to question A-M**

Question: Do you prefer corporate procurement for IT or an independent process?

Classification: Accepted M.1 – IT procurement should be a normal part of the corporate procurement process.

Deduction: It is preferred that IT procurement is a normal part of the corporate procurement process. Some organisations have a more federal structure, which allows support functions such as IT to embed procurement into its operations.  As four out of ten participants preferred this approach, it would be mentioned as an option in the framework.

Cross-reference: Recommendations 13, 21, 25

### Question A-N

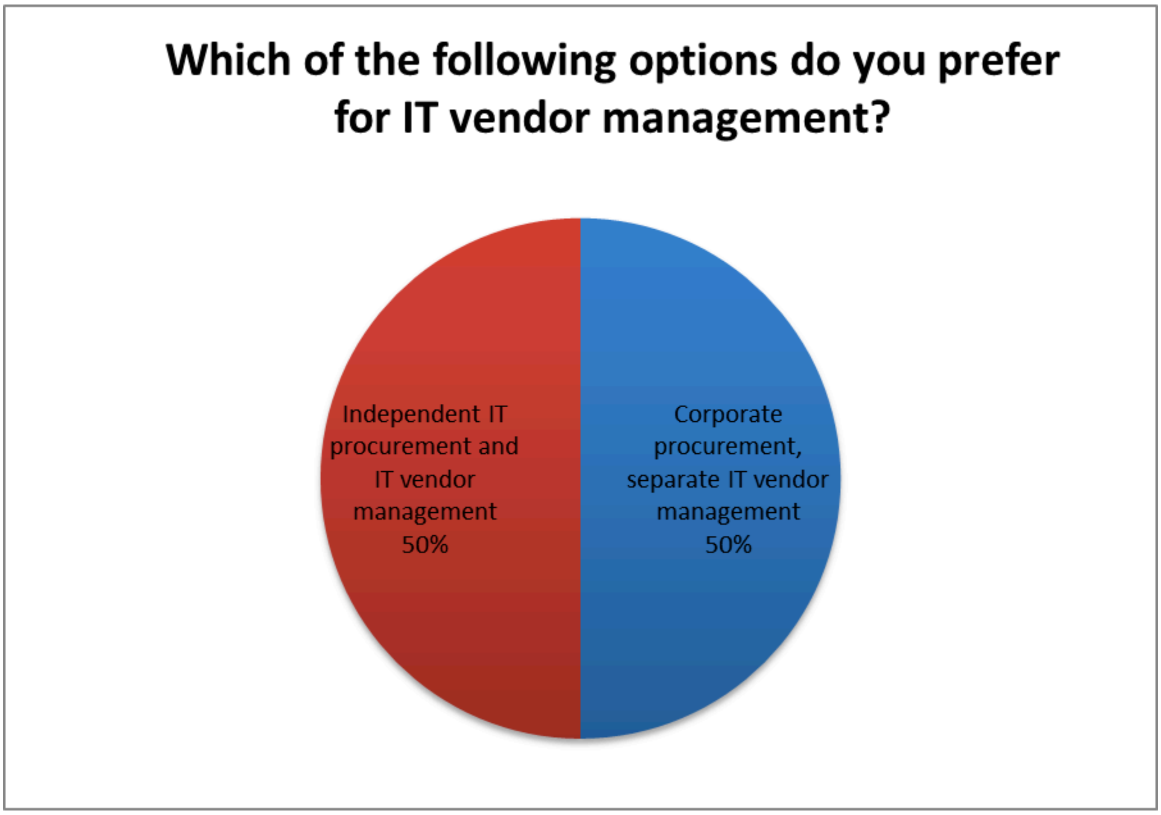


**Diagram p – Response to question A-N**

Question: Which of the following options do you prefer (please tick one) for IT vendor management?

Classification: Undecided

Deduction: Depending on the organisation, the Procurement function might handle all aspects of IT procurement and IT vendor management. This is the deduction, based on the split opinion of participants.

Cross-reference: Recommendation 13, 25

### Question A-O

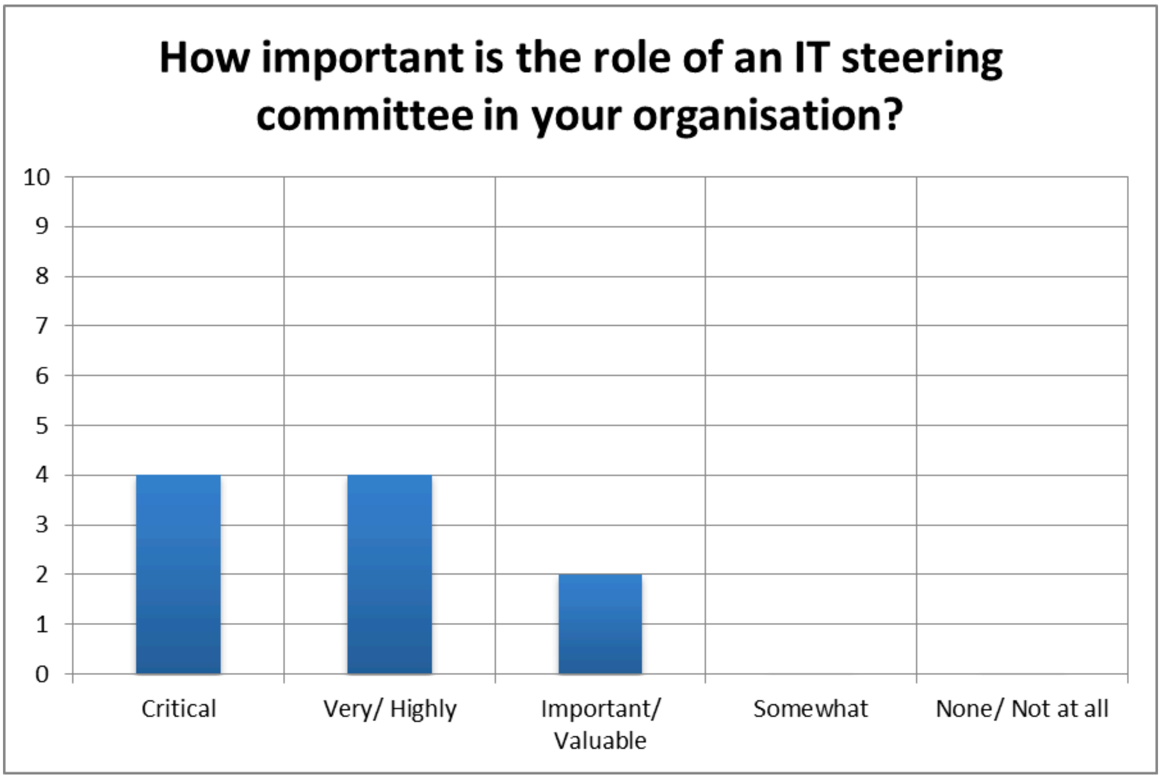


**Diagram q – Response to question A-O**

Question: How important is the role of an IT Steering Committee in your organisation?

Classification: Accepted

Deduction: An IT Steering Committee is significantly important.

Cross-reference: Recommendation 13, 31

### Question A-P

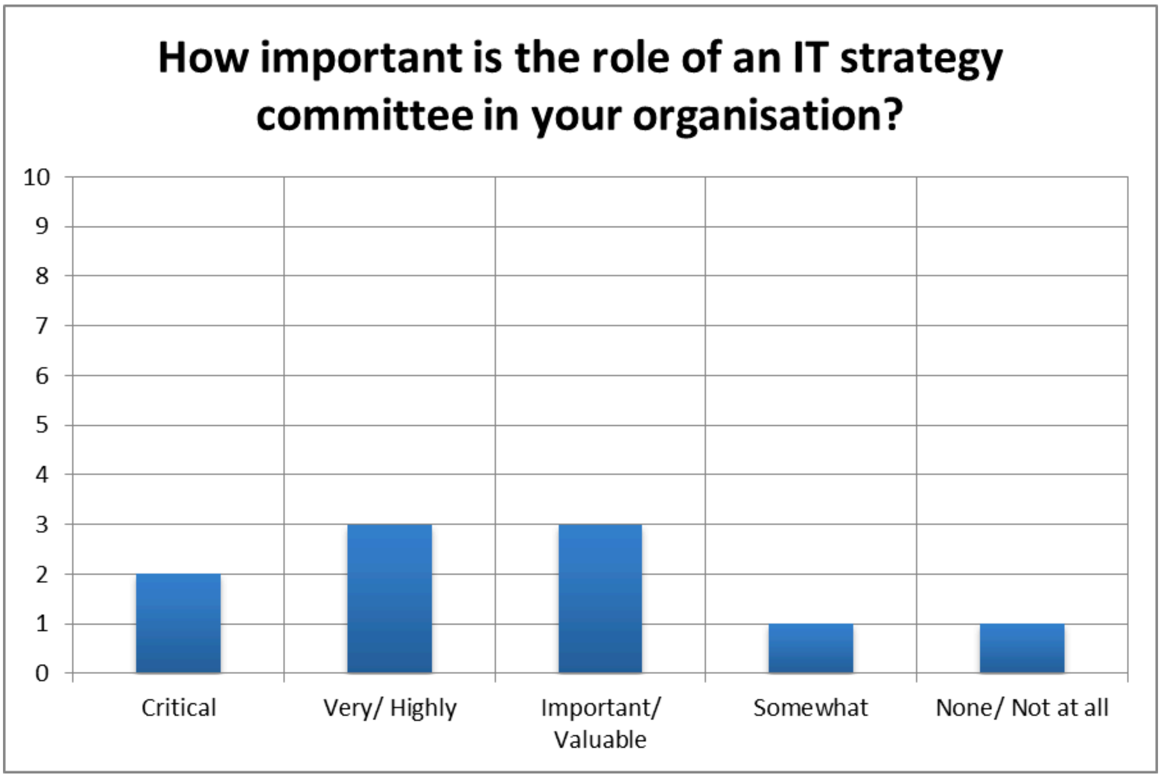


**Diagram r – Response to question A-P**

Question: How important is the role of an IT Strategy Committee in your organisation?

Classification: Accepted

Deduction: An IT Strategy Committee is significantly important, yet non-structured input by participants suggested that there is a preference to combine the IT Strategy Committee and IT Steering Committee.

Cross-reference: Recommendation 30

### Question A-Q

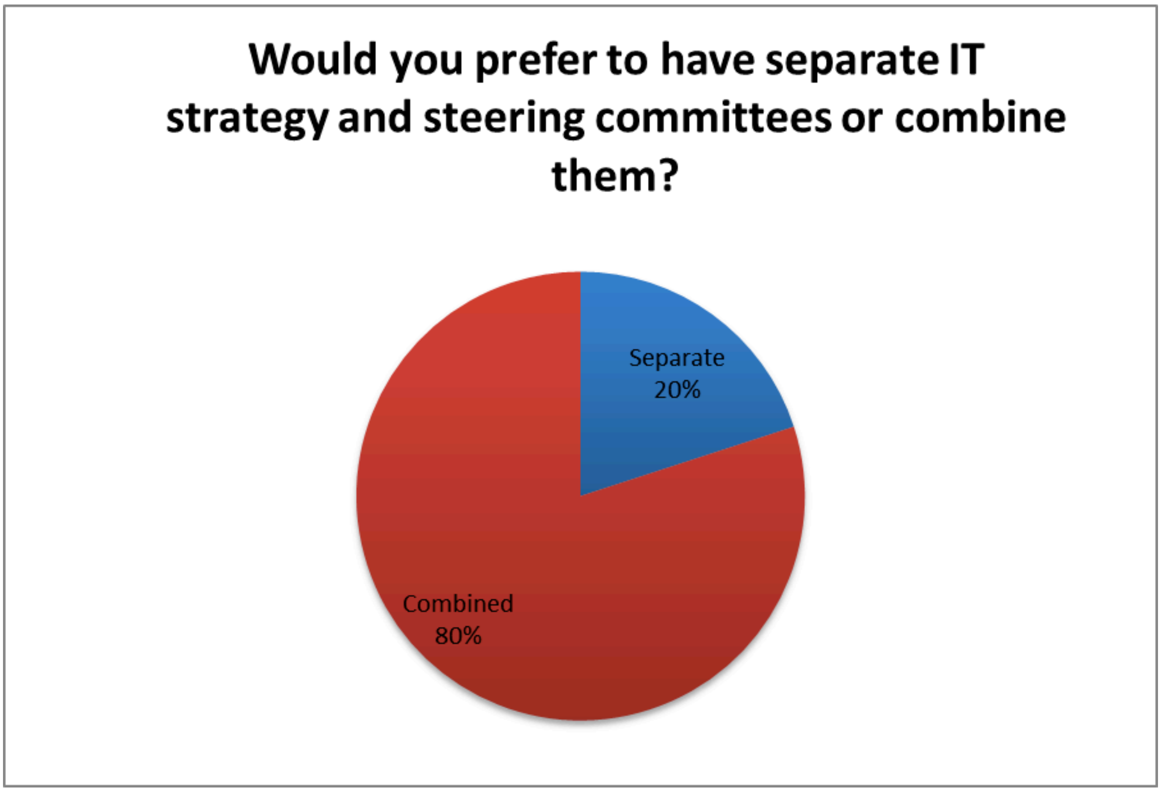


**Diagram s – Response to question A-Q**

Question: Would you prefer to have separate IT Strategy and Steering Committees or combine them? Please tick one option.

Classification: Accepted – A-Q.2 – A combined IT Steering and Strategy Committee is preferred.

Deduction: The preferred approach is to combine the IT strategy role with that of the IT Steering Committee, which was also confirmed by the non-structured input.

Cross-reference: Recommendations 30, 31

### Question A-R

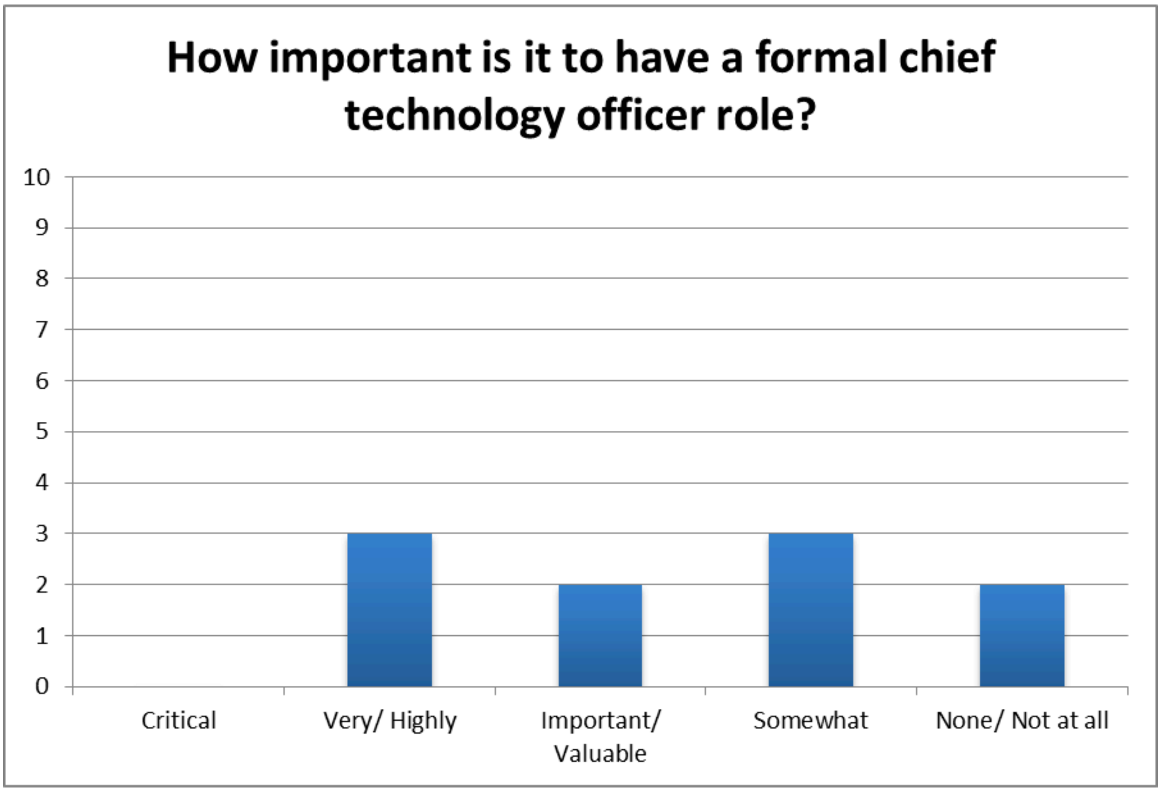


**Diagram t – Response to question A-R**

Question: How important is it to have a formal chief technology officer (CTO) role?

Classification: Considered

Deduction: The CTO role is useful but not of high importance.  This is in line with the researcher's experience in the public and private sectors of South Africa, where few organisations have a formal CTO role.

Cross-reference: Recommendations 21, 22

### Question A-S

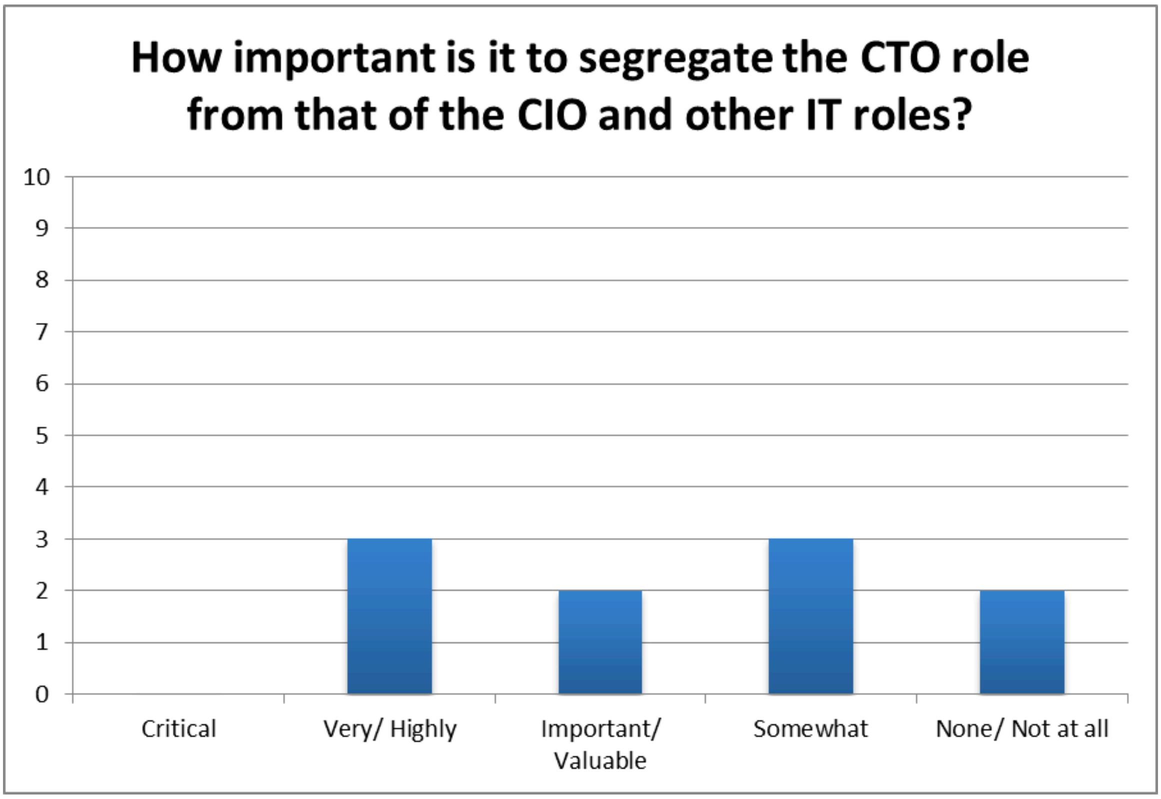


**Diagram u – Response to question A-S**

Question: How important is it to segregate the CTO role from that of the CIO and other IT roles?

Classification: Considered

Deduction: It is not highly important to segregate the CIO and CTO roles. Considering the response to the preceding question, this is not surprising.

Cross-reference: Recommendations 21, 22

### Question A-T

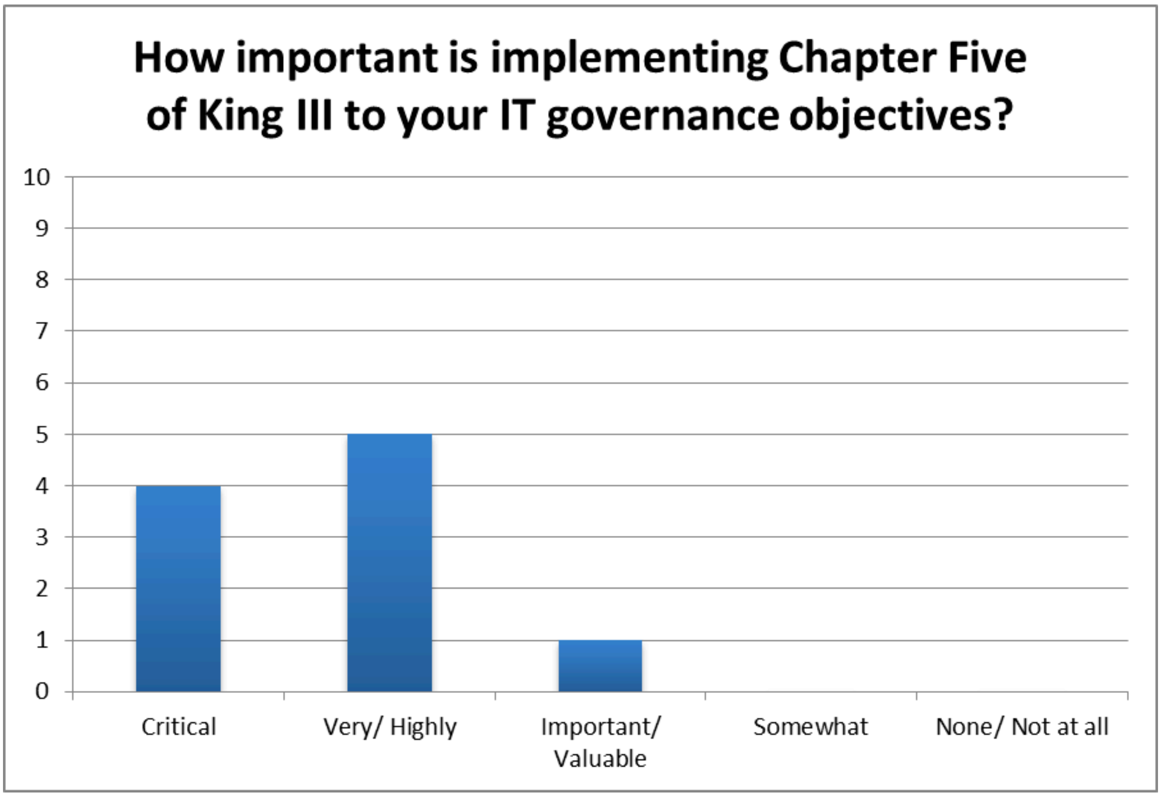


**Diagram v – Response to question A-T**

Question: How important is implementing the IT governance chapter of the King III Code of Corporate Governance to your IT governance objectives?

Classification: Accepted

Deduction: It is of significant importance to implement Chapter 5 of King III.

Cross-reference: Recommendation 13

### Question A-U

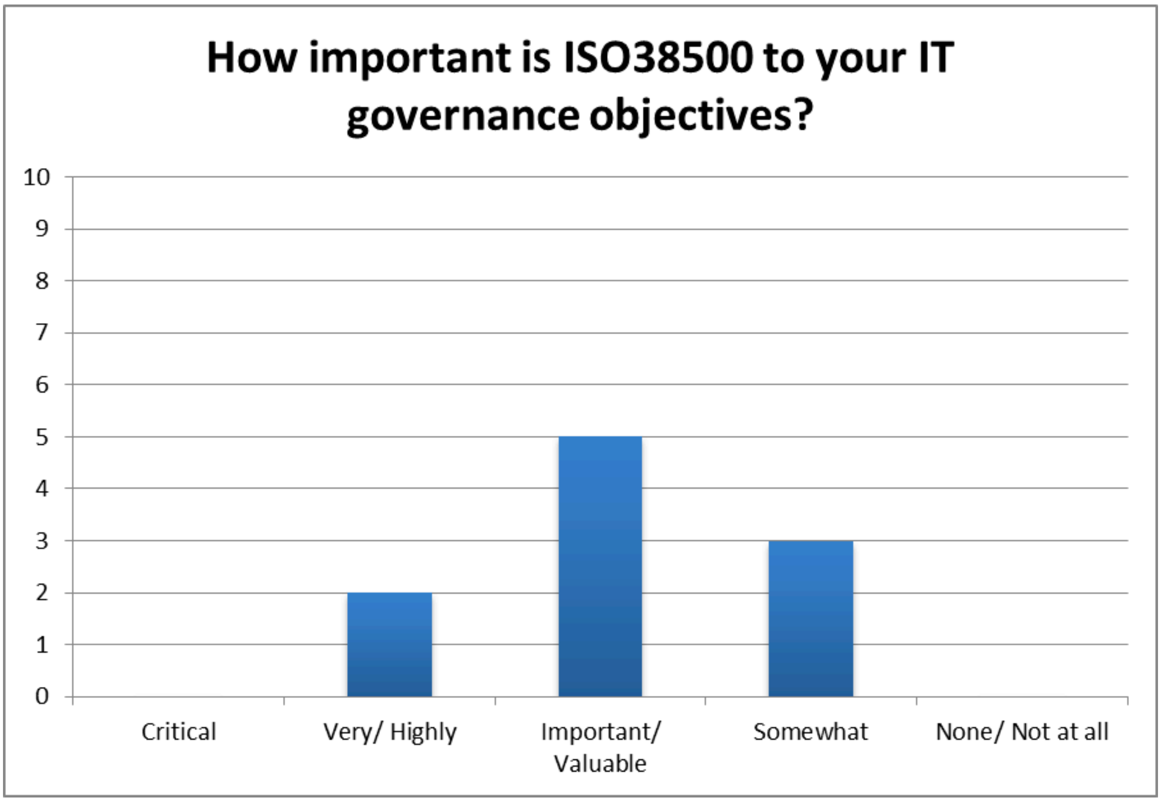


**Diagram w – Response to question A-U**

Question: How important is implementing the concepts of the ISO/IEC38500 IT governance standard to your IT governance objectives?

Classification: Considered

Deduction: It is not highly important to implement ISO/IEC38500. The formal take-up of ISO/IEC38500 has been low, but the IT governance investments driven by King III Chapter Five implementations, as well as limited interest in COBIT 5, which has incorporated many aspects of ISO/IEC38500, suggests indirect adoption of the standard.

Cross-reference: Recommendation 14

## B. Strategic alignment

### Questions B-A to B-E combined

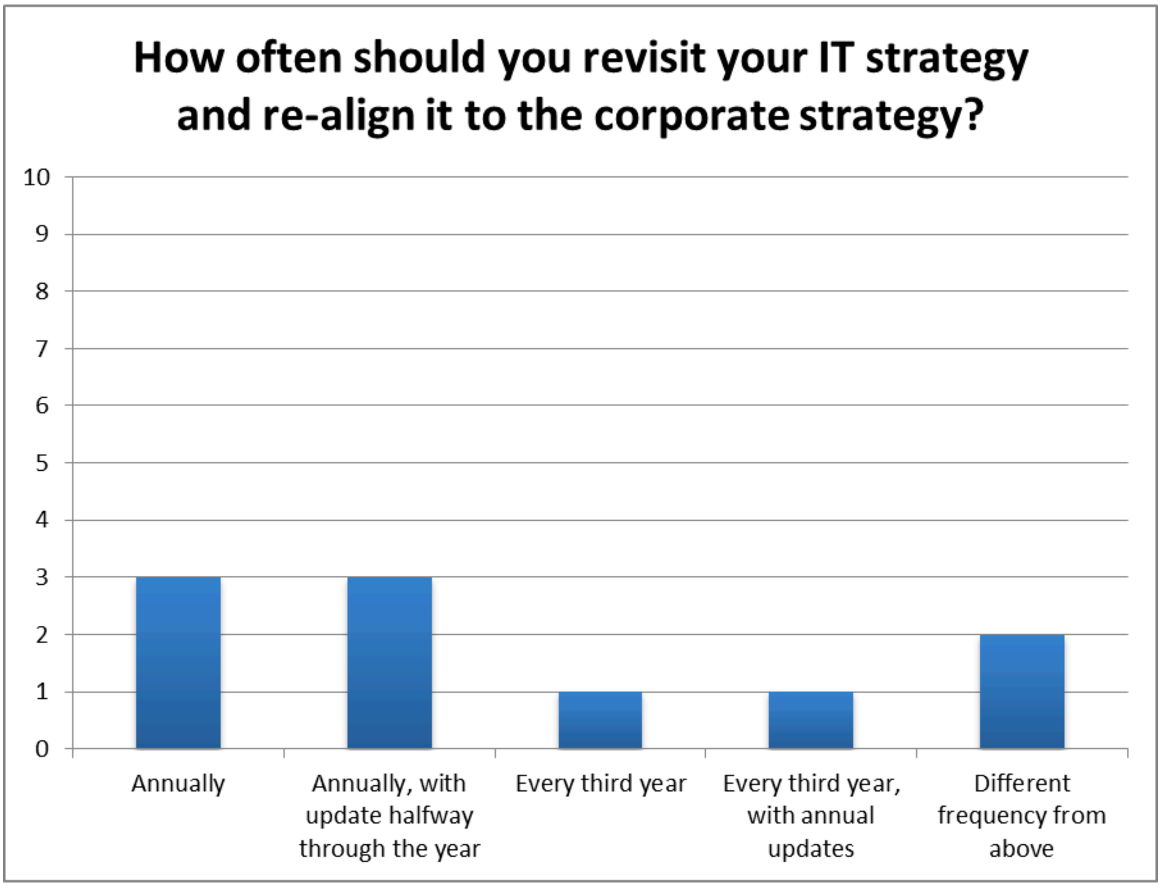


**Diagram x – Response to questions B-A to B-E**

Question: How often should you revisit your IT strategy and re-align it to the corporate strategy?

Classification: Not accepted

Deduction: IT strategy should be updated at least annually, with consideration given to an update midway through the year. There was consensus that an update should take place at least annually, but some participants felt that updates should be made whenever business change requires, even if at irregular intervals throughout the year.

Cross-reference: Recommendation 1

### Questions B-F to B-K

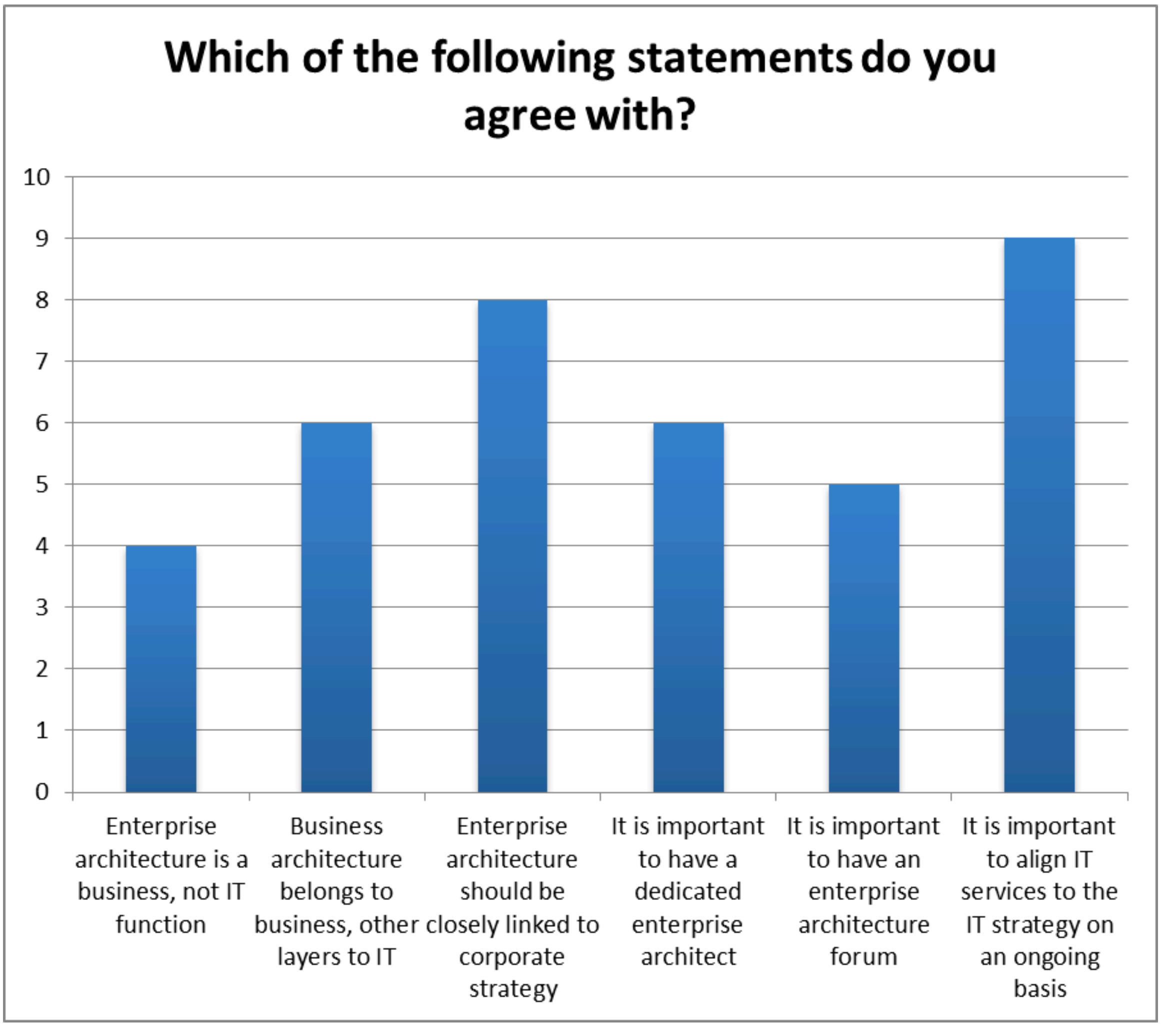


**Diagram y – Response to questions B-F to B-K**

Question: Which of the following statements do you agree with?

Classification: B-F – Not accepted; B-G to I, K – Accepted; B-J – Considered

Deduction:

- B-G: The business architecture belongs to business, the remaining architecture layers belong to the IT function.
- B-H: Enterprise architecture should be closely linked to the corporate strategy function, to translate strategy into action.
- B-I: Despite indications that a dedicated enterprise architect role is required, non-structured input indicated that the IT architect role should be emphasised instead.
- B-J: Based on non -trutcured input, it was decided to rather emphasise the importance of a technology architecture forum.
- B-K: It is important to align IT services to the IT strategy on an ongoing basis.

Cross-reference: Recommendations 1, 11, 18, 19, 24, 32

### Question B-L

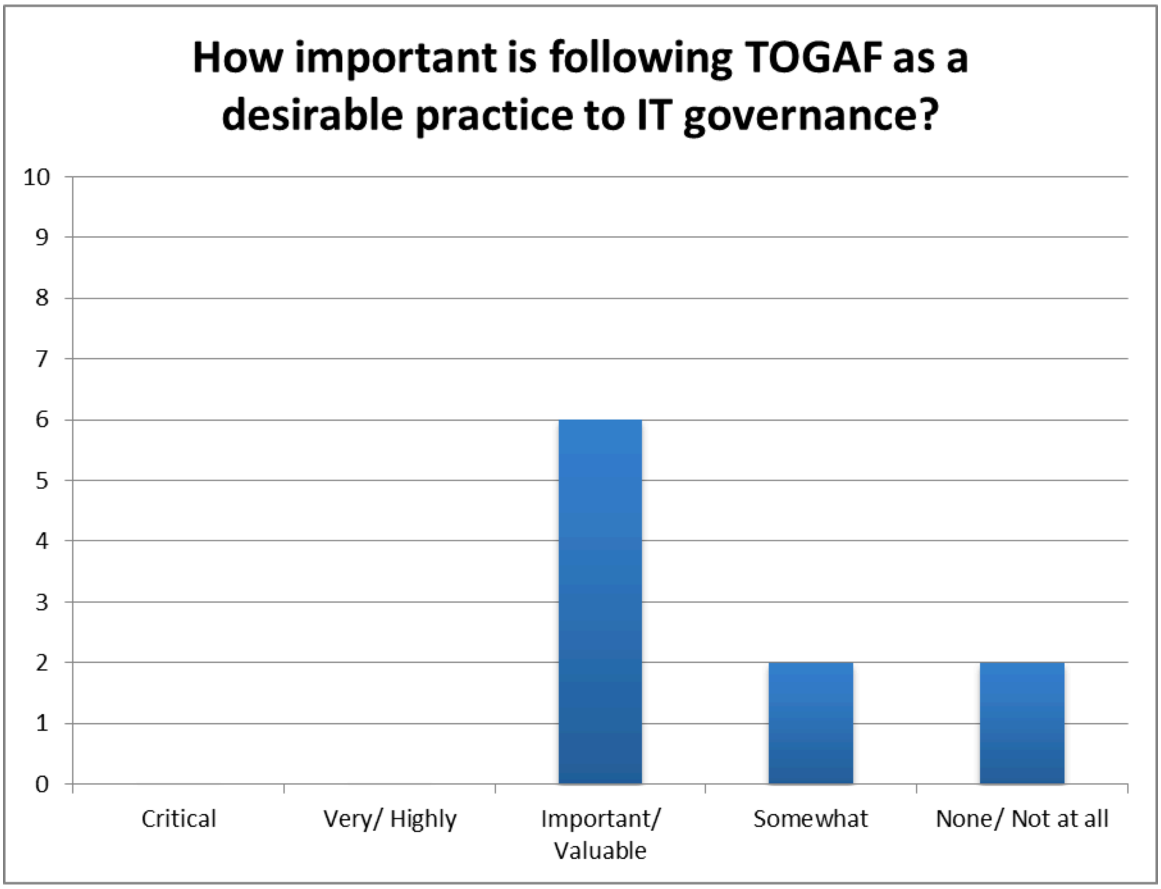


**Diagram z – Response to question B-L**

Question: How important is the following to practising sound IT governance? Following TOGAF as a desirable practice.

Classification: Considered

Deduction: Non-structured feedback about TOGAF adoption suggested that the participants do not want to be limited to TOGAF. Nobody objected to TOGAF, but would prefer to use a variety of architecture standards, methods and tools, rather than being limited to one.

Cross-reference: Recommendation 11

### Question B-M

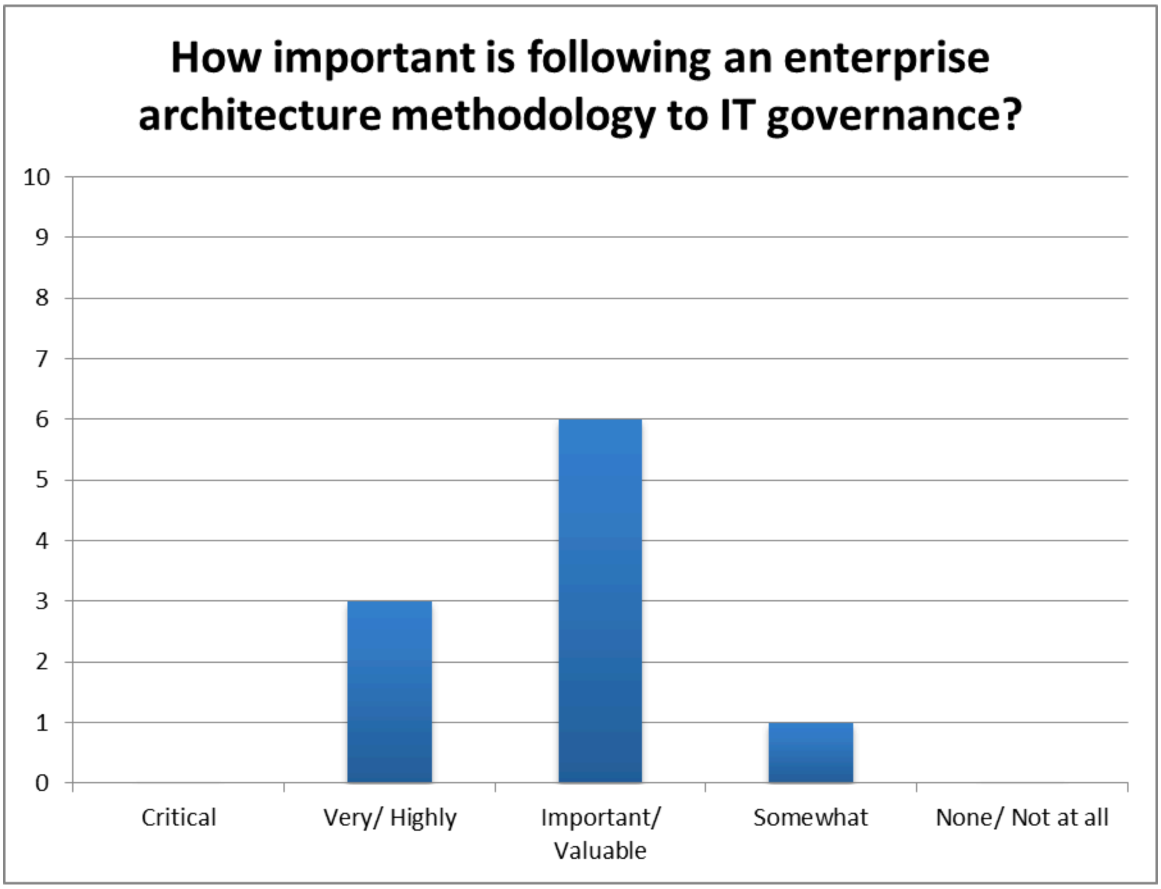


**Diagram aa – Response to question B-M**

Question: How important is the following to practising sound IT governance? Following an enterprise architecture methodology, regardless of the adopted practice.

Classification: Considered

Deduction: Non-structured feedback indicated that participants believe IT architecture should be an IT responsibility but that business should be responsible for the other layers of the enterprise architecture.

Cross-reference: Recommendation 11

### Question B-N

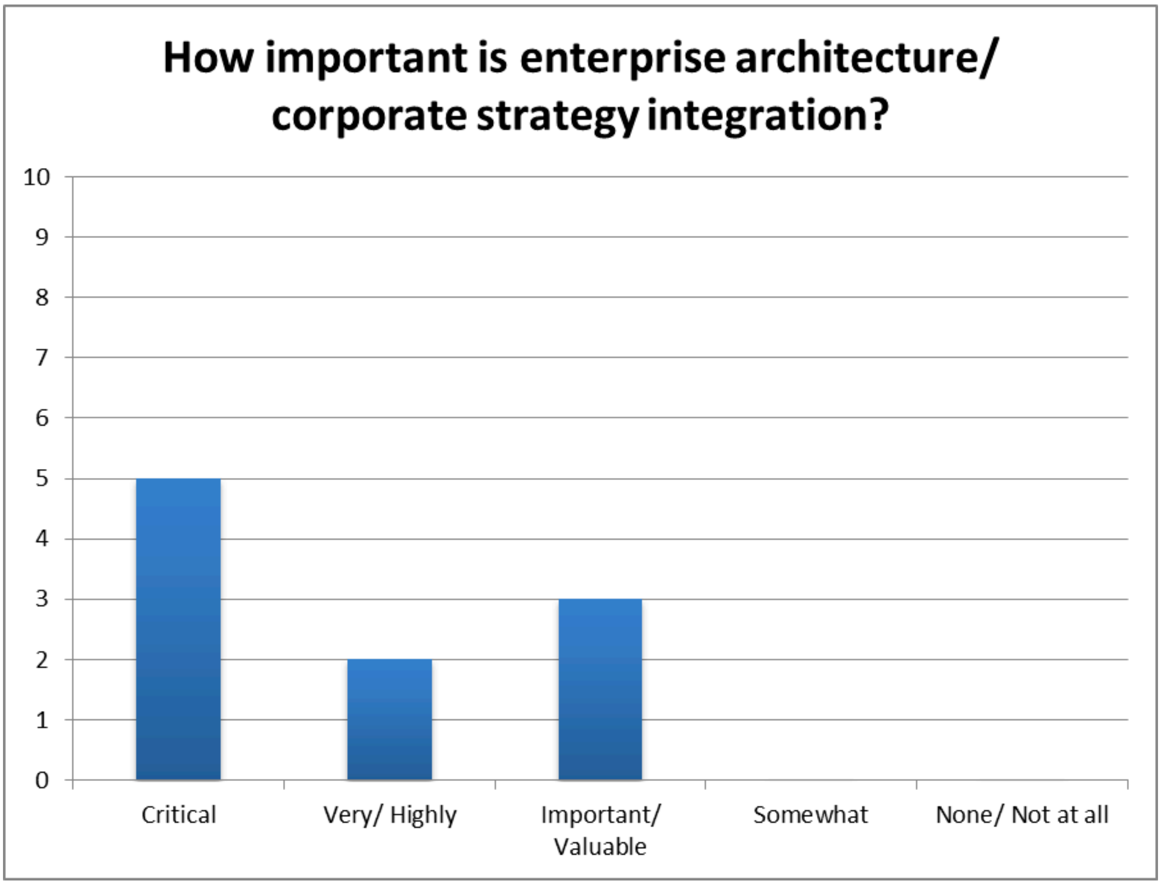


**Diagram ab – Response to question B-N**

Question: How important is the following to practising sound IT governance? Integration between enterprise architecture and corporate strategy.

Classification: Accepted

Deduction: Integration between corporate strategy and enterprise architecture is of significant importance. This suggests that the IT strategy and IT architecture integration is also significantly important.

Cross-reference: Recommendation 32

## C. Value delivery

### Question C-A

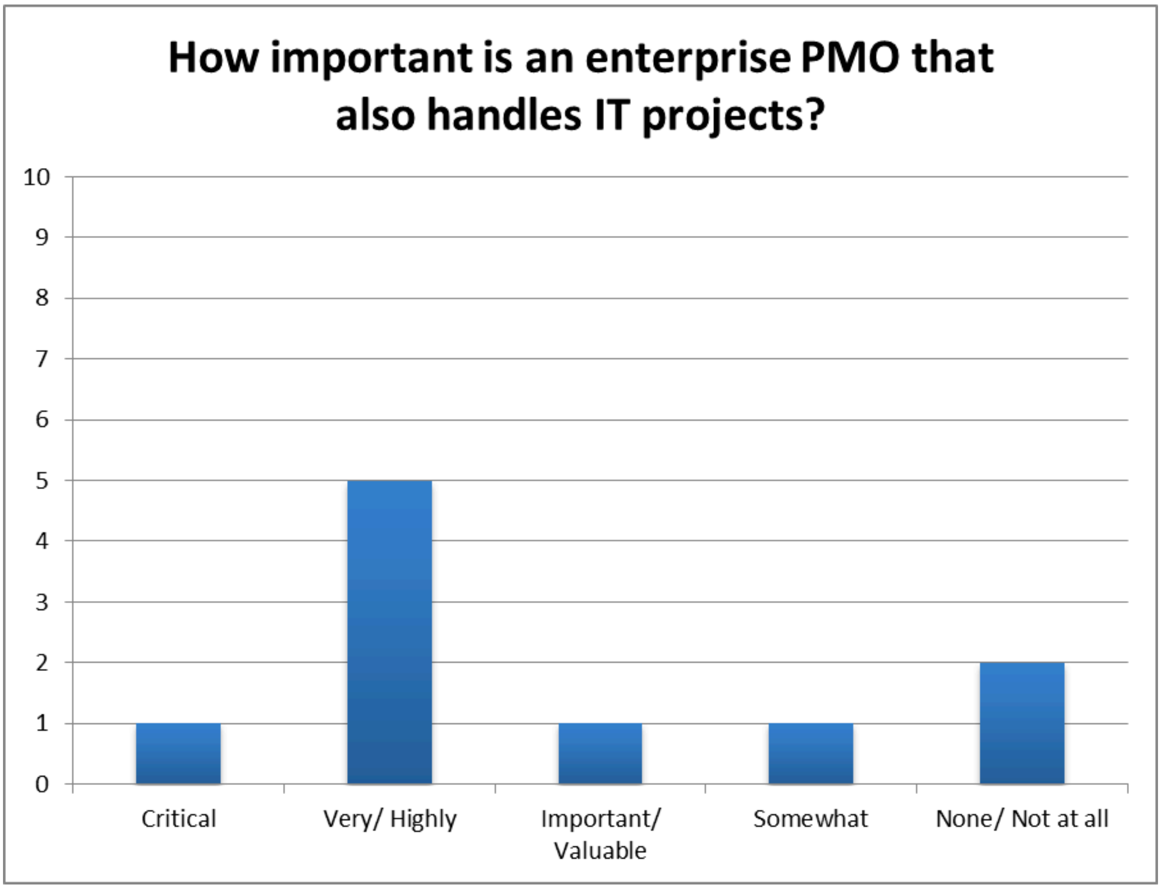


**Diagram ac – Response to question C-A**

Question: How important is each of the following to sound value delivery in your organisation? Having an enterprise PMO that also handles IT projects.

Classification: Accepted

Deduction: An enterprise PMO with responsibility for handling IT projects is of importance.

Cross-reference: Recommendation 33

### Question C-B

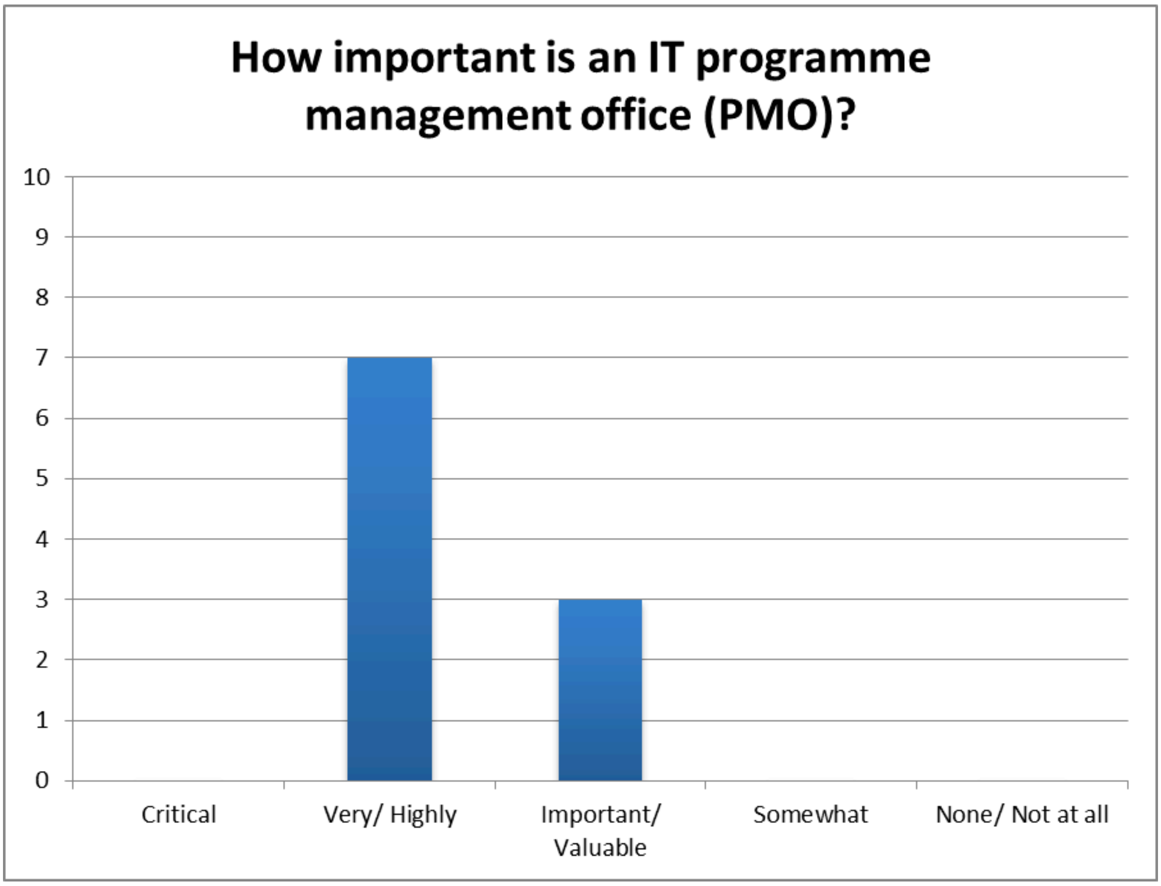


**Diagram ad – Response to question C-B**

Question: How important is each of the following to sound value delivery in your organisation? Having an IT PMO, regardless of whether an enterprise PMO exists or not.

Classification: Accepted

Deduction: It is important to incorporate the IT PMO into the IT governance structures, regardless of whether this is a standalone PMO or part of the enterprise PMO. This and the preceding question overlap and could have been structured better.

Cross-reference: Recommendation 33

## Question C-C

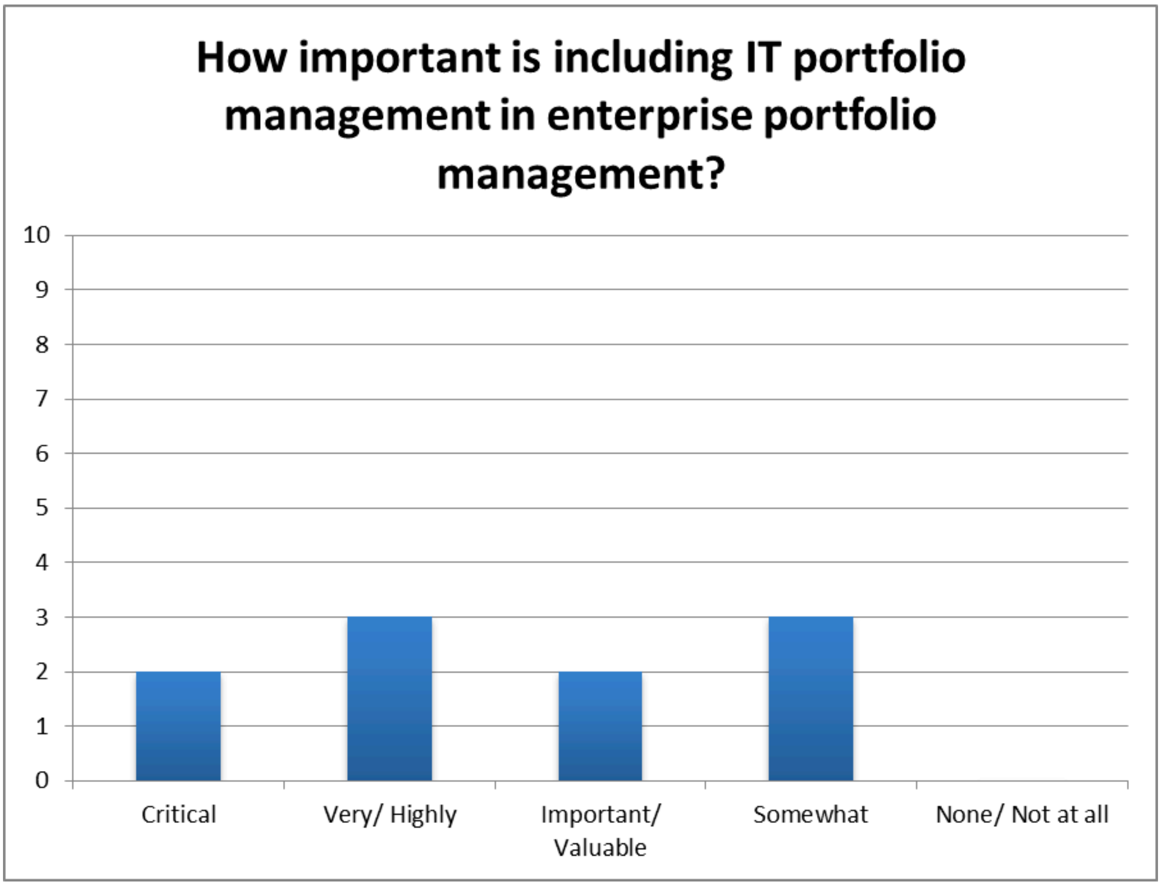


**Diagram ae – Response to question C-C**

Question: How important is each of the following to sound value delivery in your organisation? Including IT portfolio management in enterprise portfolio management?

Classification: Accepted

Deduction: IT portfolio management is of importance to enterprise portfolio management.

Cross-reference: Recommendation 19

### Question C-D

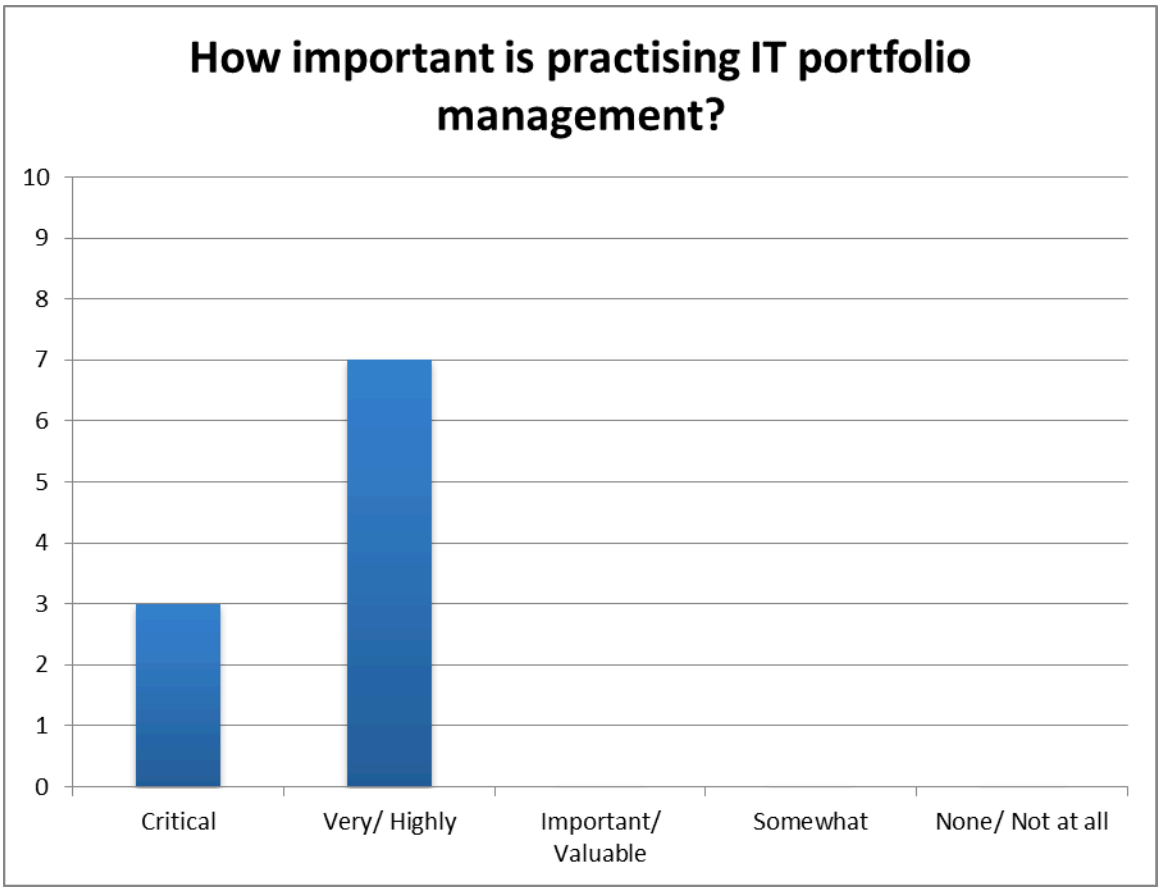


**Diagram af – Response to question C-D**

Question: How important is each of the following to sound value delivery in your organisation? Practising IT portfolio management, regardless of whether enterprise portfolio management is practised or not.

Classification: Accepted

Deduction: IT portfolio management is of significant importance. Again , the question overlaps with its predecessor.

Cross-reference: Recommendation 19

### Question C-E

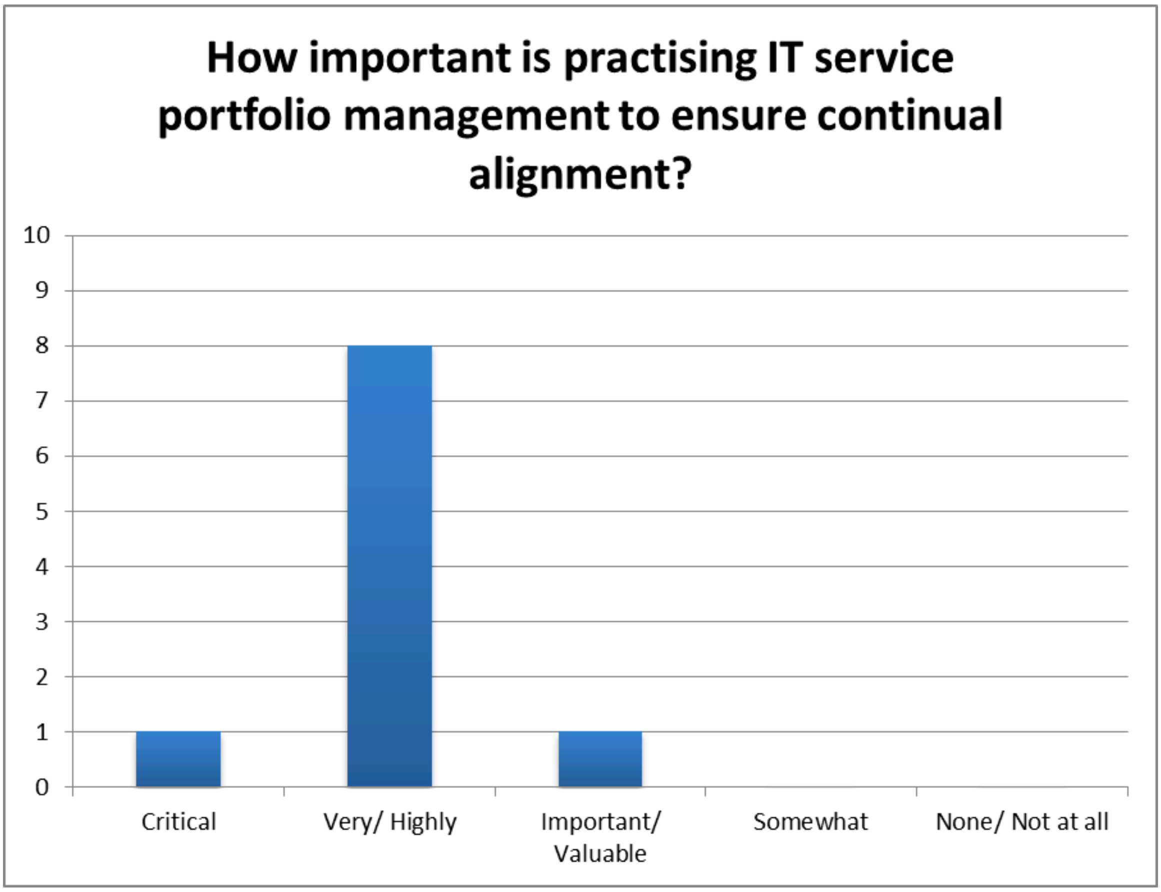


**Diagram 7.ag – Response to question C-E**

Question: How important is each of the following to sound value delivery in your organisation? Practising IT service portfolio management to ensure continual alignment of services to the organisational strategy.

Classification: Accepted

Deduction: IT service portfolio management is significantly important for the continual alignment of IT services to business needs.

Cross-reference: Recommendation 19

### Question C-F

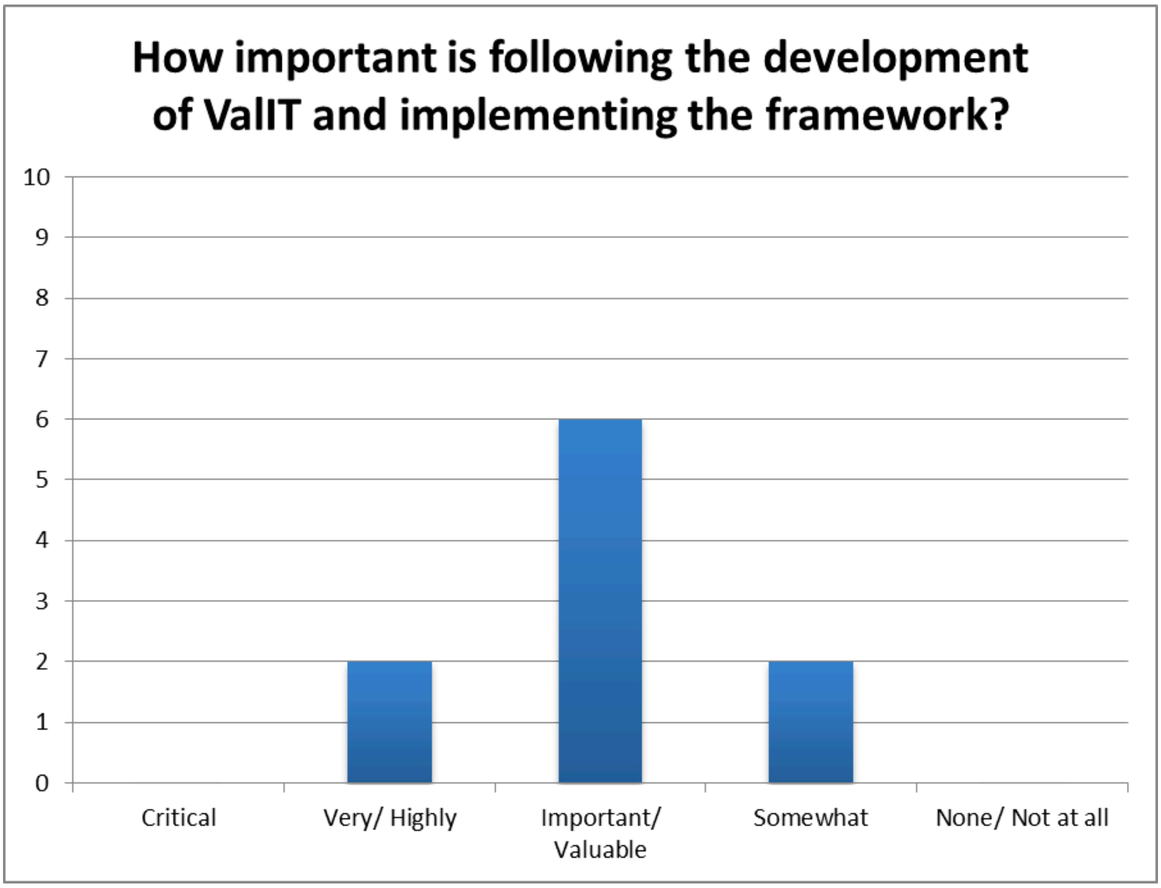


**Diagram ah – Response to question C-F**

Question: How important is each of the following to sound value delivery in your organisation? Following the development of ValIT and implementing the framework once it has matured sufficiently.

Classification: Considered

Deduction: Most participants have not yet taken notice of ValIT, although IT value management is a general problem, in the researcher's experience.  ValIT has since been incorporated into COBIT 5, the take-up of which has also not been high in South Africa.

Cross-reference: Recommendations 2, 7, 19, 20

### Question C-G

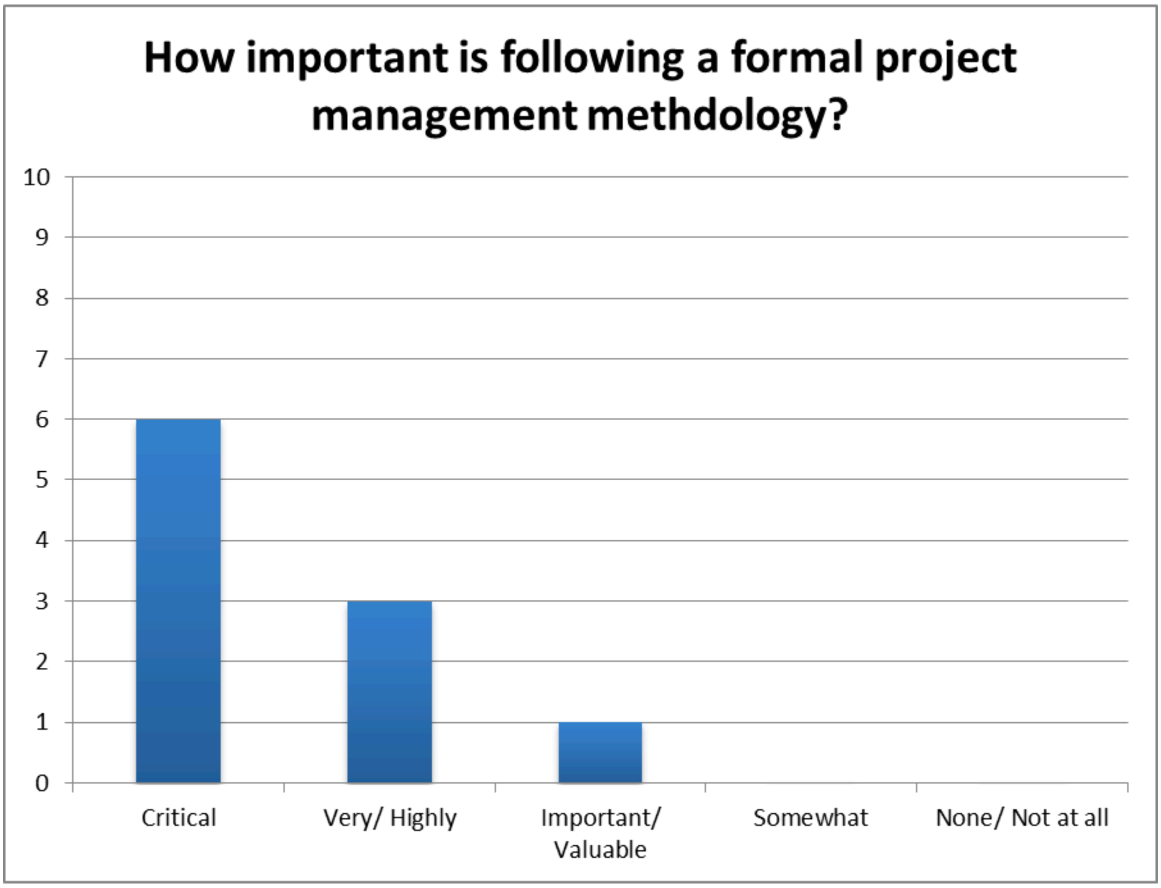


**Diagram ai – Response to question C-G**

Question: How important is each of the following to sound value delivery in your organisation? Following a formal project management methdology

Classification: Accepted

Deduction: Adoption of a formal project management methodology is significantly important to sound value delivery.

Cross-reference: Recommendations 3, 10, 14, 34

## Question C-H

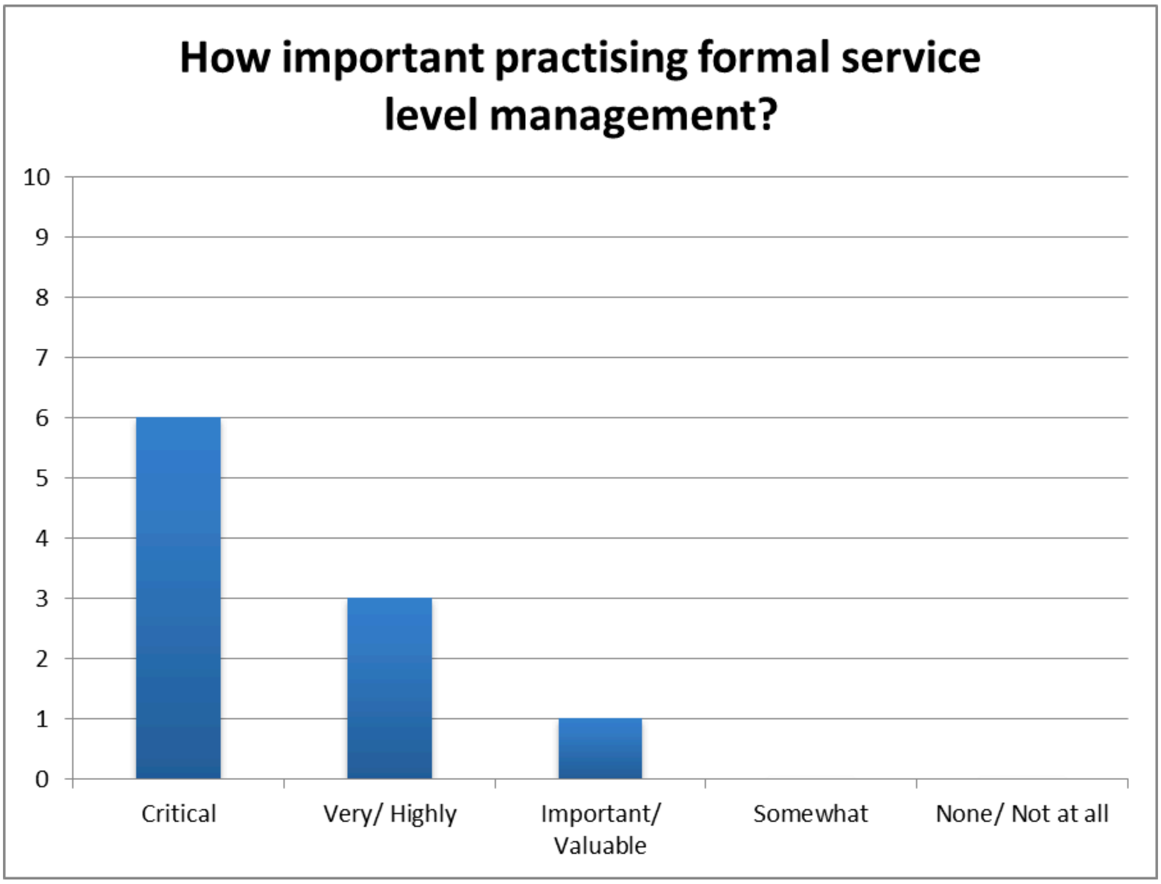


**Diagram aj – Response to question C-H**

Question: How important is each of the following to sound value delivery in your organisation? Practising formal service level management.

Classification: Accepted

Deduction: Adoption of formal service level management is significantly important to sound value delivery in the organisation.

Cross-reference: Recommendations 2, 3

### Question C-I

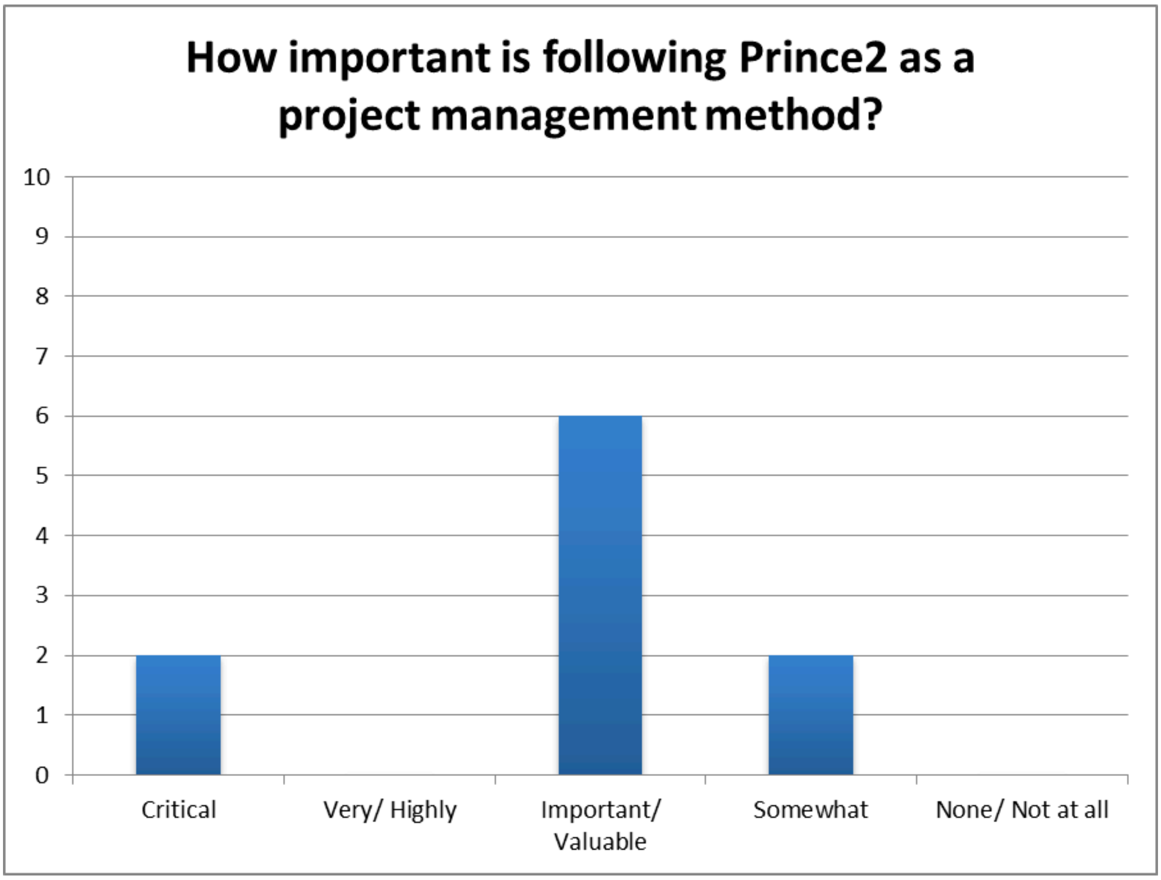


**Diagram ak – Response to question C-I**

Question: How important is each of the following to sound IT governance in your organisation? Following Prince2 as a project management method.

Classification: Considered

Deduction: Considering the earlier PMO-related responses, the governance over projects is more important than the method adopted, in this instance Prince2.

Cross-reference: Recommendation 10

### Question C-J

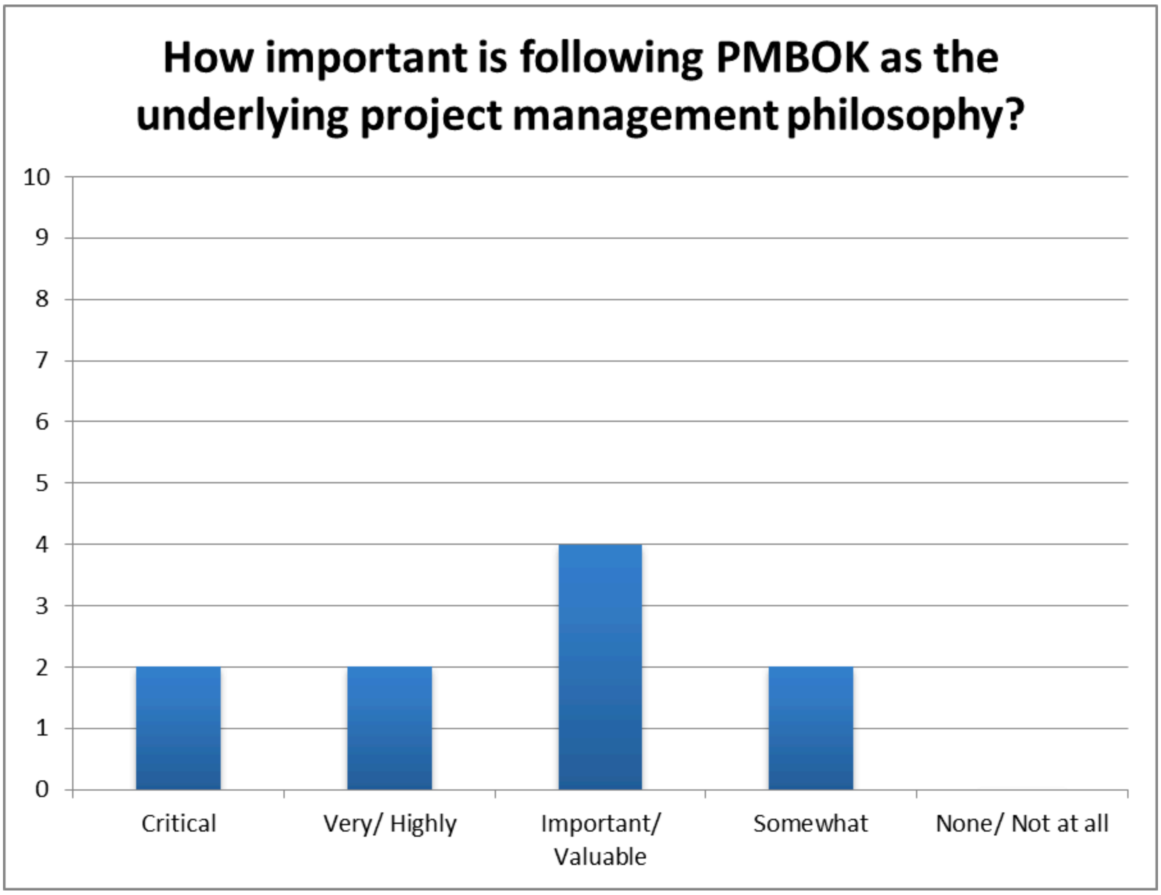


**Diagram al – Response to question C-J**

Question: How important is each of the following to sound IT governance in your organisation? Following PMBOK as the underlying project management philosophy, regardless of what other methodologies are used.

Classification: Considered

Deduction: Again, the governance over projects is more important than the methods (Prince2) or philosophy (PMBOK).

Cross-reference: Recommendation 10

### Question C-K

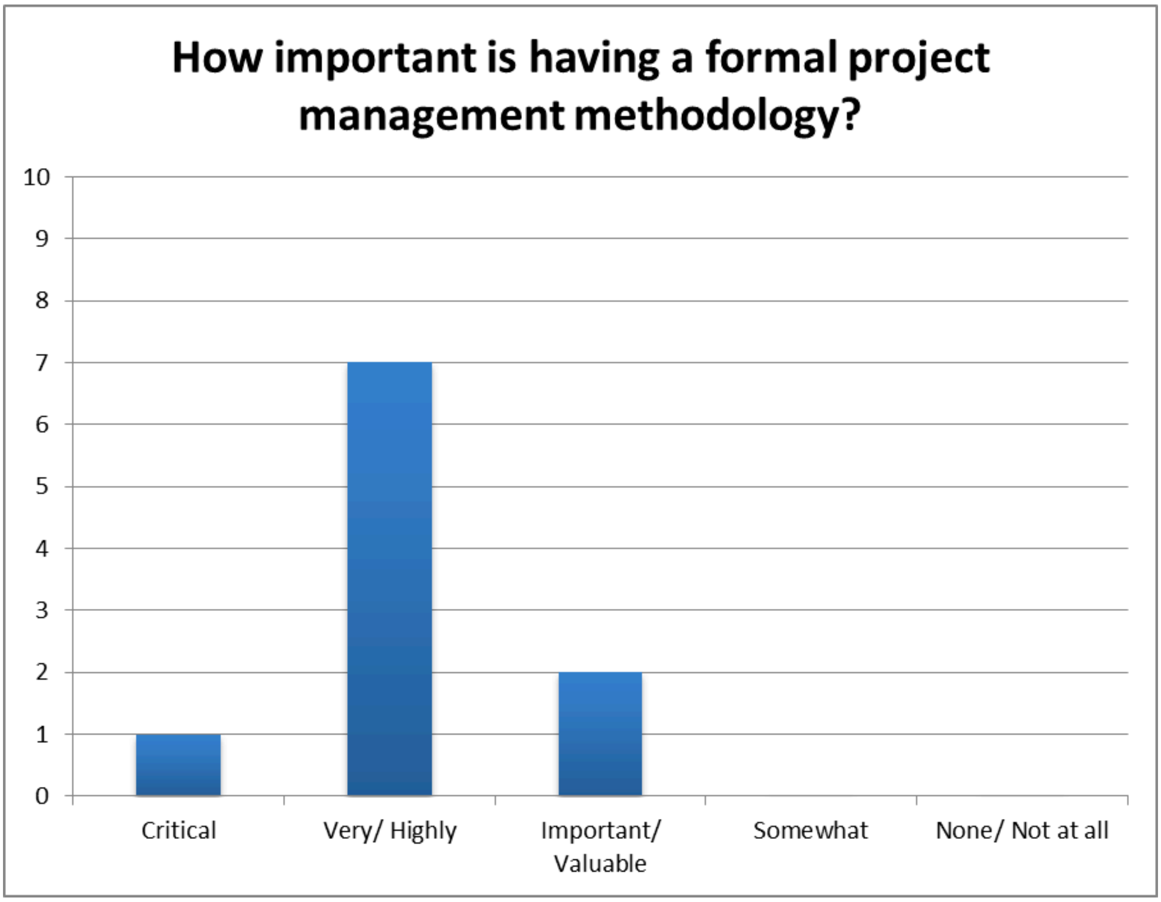


**Diagram am – Response to question C-K**

Question: How important is each of the following to sound IT governance in your organisation? Having any formal project management methodology, regardless of whether it is Prince2.

Classification: Accepted

Deduction: Grouped with the PMO under the project governance category, it is significantly important to have a formal project management methodology; more important than the method (Prince2) or philosophy (PMBOK).

Cross-reference: Recommendation 10

## Question C-L

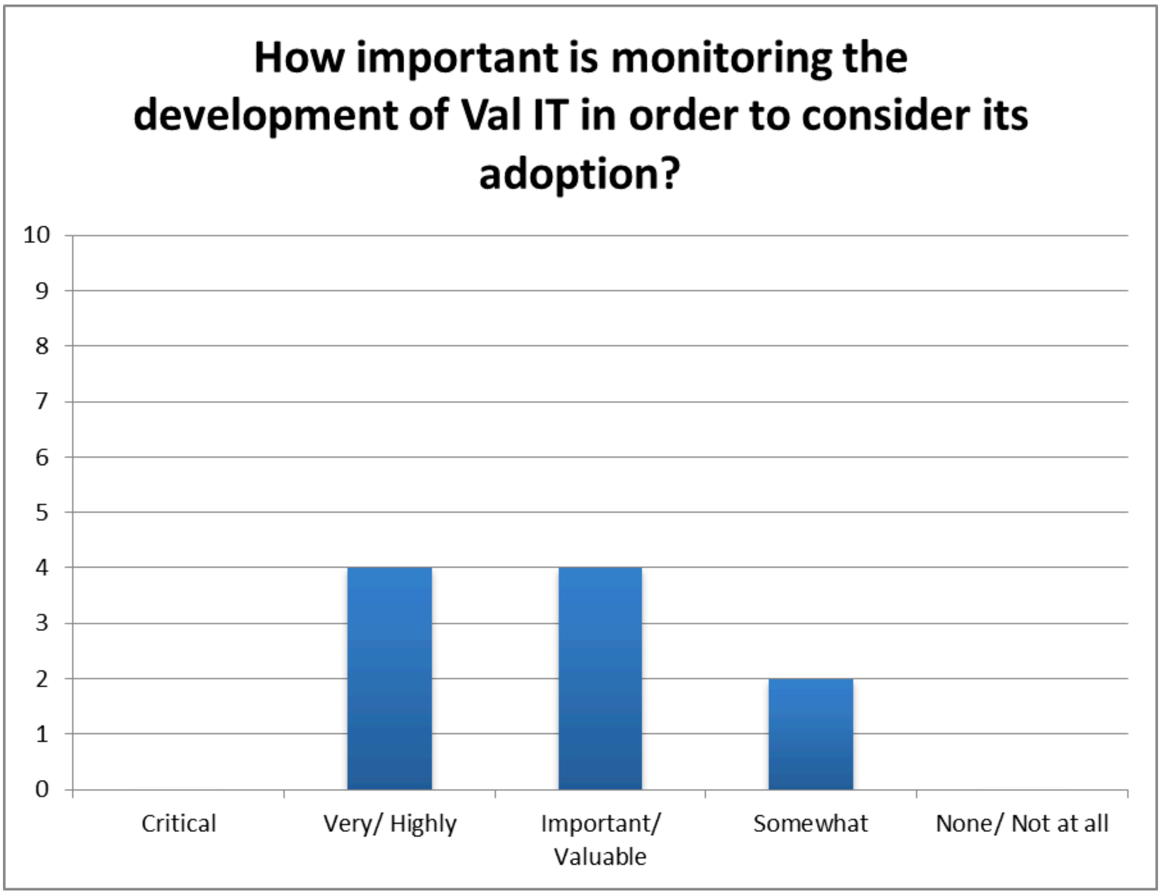


**Diagram an – Response to question C-L**

Question: How important is each of the following to sound IT governance in your organisation? Monitoring the development of ValIT as a value mangement practice, in order to consider its adoption once it has matured sufficiently.

Classification: Considered

Deduction: As explained earlier, the exposure of the participants to ValIT has been low, so this response is not surprising.

Cross-reference: Recommendations 2, 7, 19, 20

## D. Resource management

### Question D-A

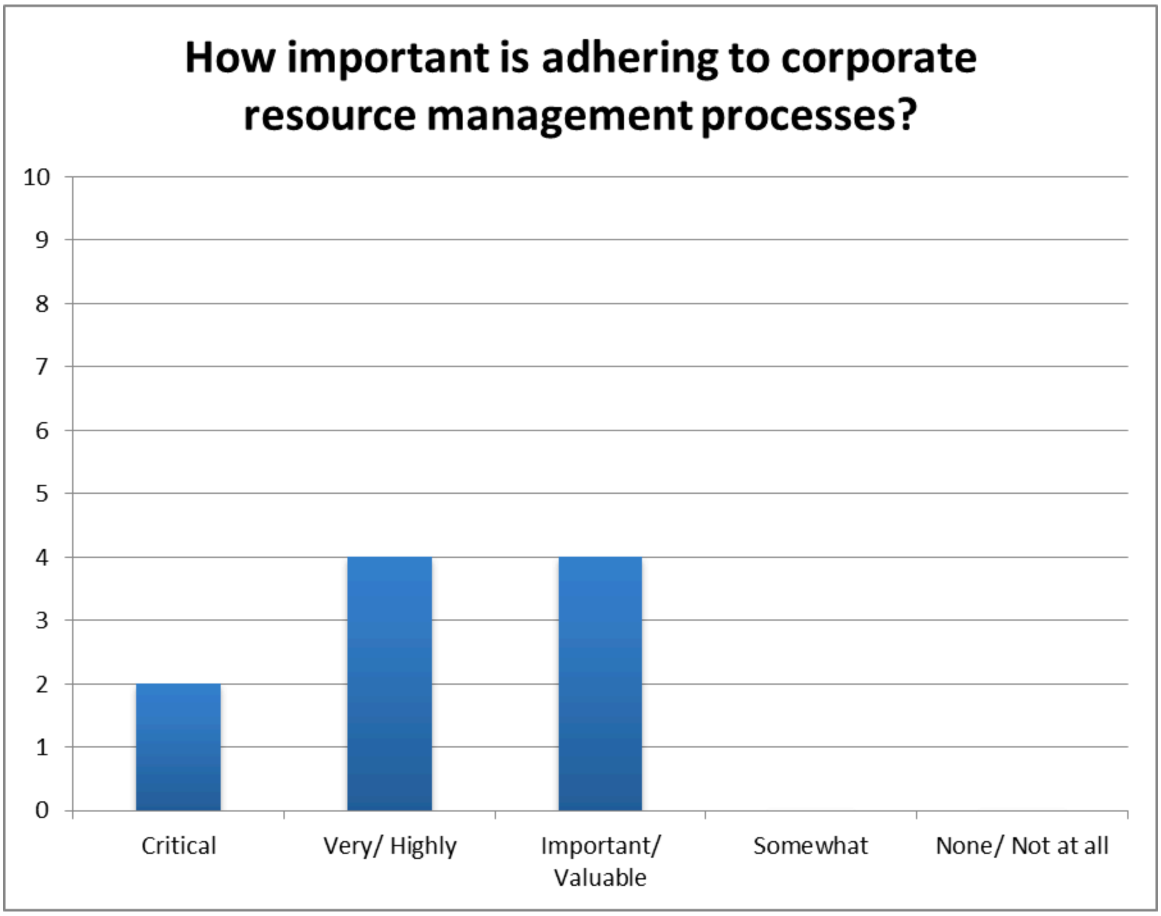


**Diagram ao – Response to question D-A**

Question: How important is each of the following to sound IT resource management in your organisation? Adhering to corporate resource management processes, as part of practising IT governance.

Classification: Accepted

Deduction: It is of importance to for IT to adhere to corporate resource management processes.

Cross-reference: Recommendation 3

### Question D-B

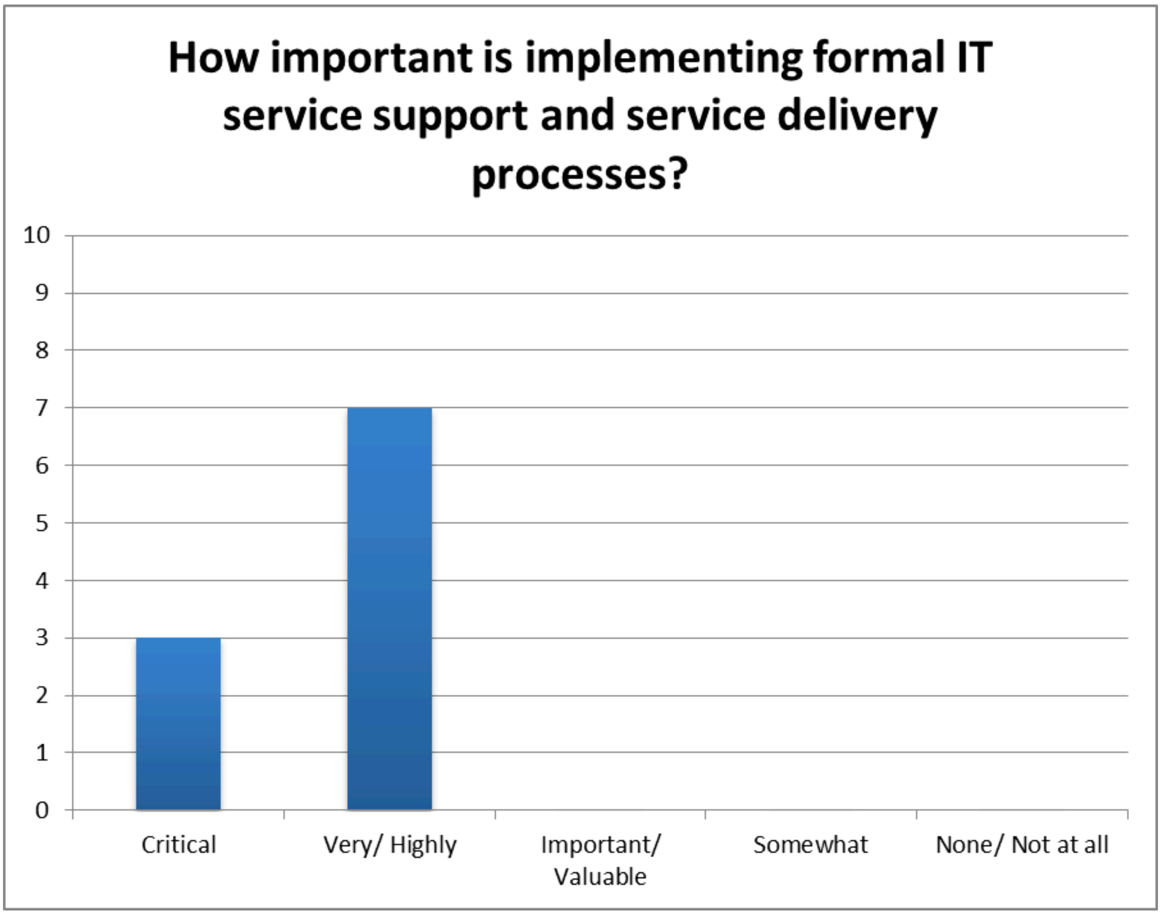


**Diagram ap – Response to question D-B**

Question: How important is each of the following to practising sound IT resource management in your organisation?  Implementing formal IT service support and service delivery processes.

Classification: Accepted

Deduction: It is significantly important to implement formal IT service support and delivery processes.

Cross-reference: Recommendation 6

### Question D-C

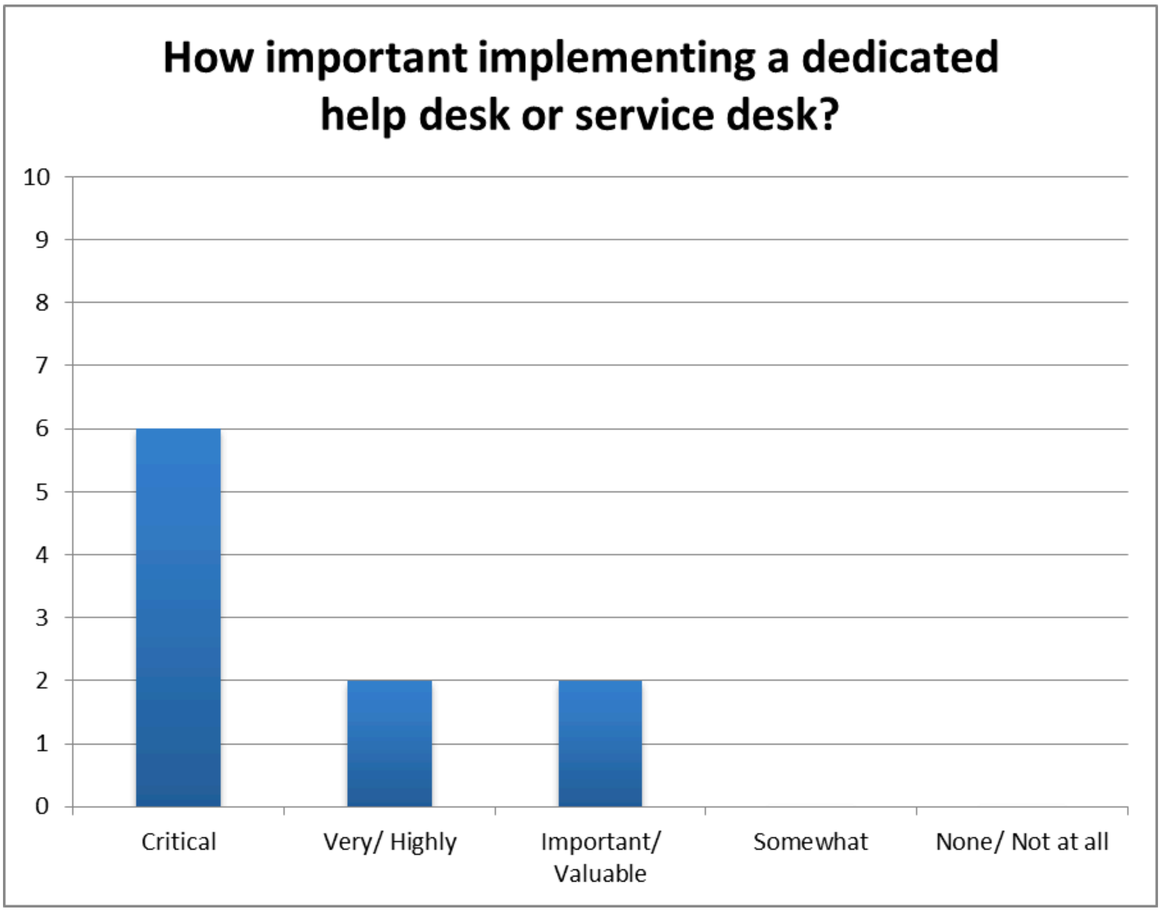


**Diagram aq – Response to question D-C**

Question: How important is each of the following to practising sound IT resource management in your organisation? Implementing a dedicated help dek or service desk.

Classification: Accepted

Deduction: It is significantly important to implement a dedicated help desk or service desk to facilitate effective IT service management.

Cross-reference: Recommendation: Non-specific. This aspect was toned down, as it is a more operational rather than governance consideration. ITIL is still recommended, which implies the implementation of a service desk.

### Question D-D

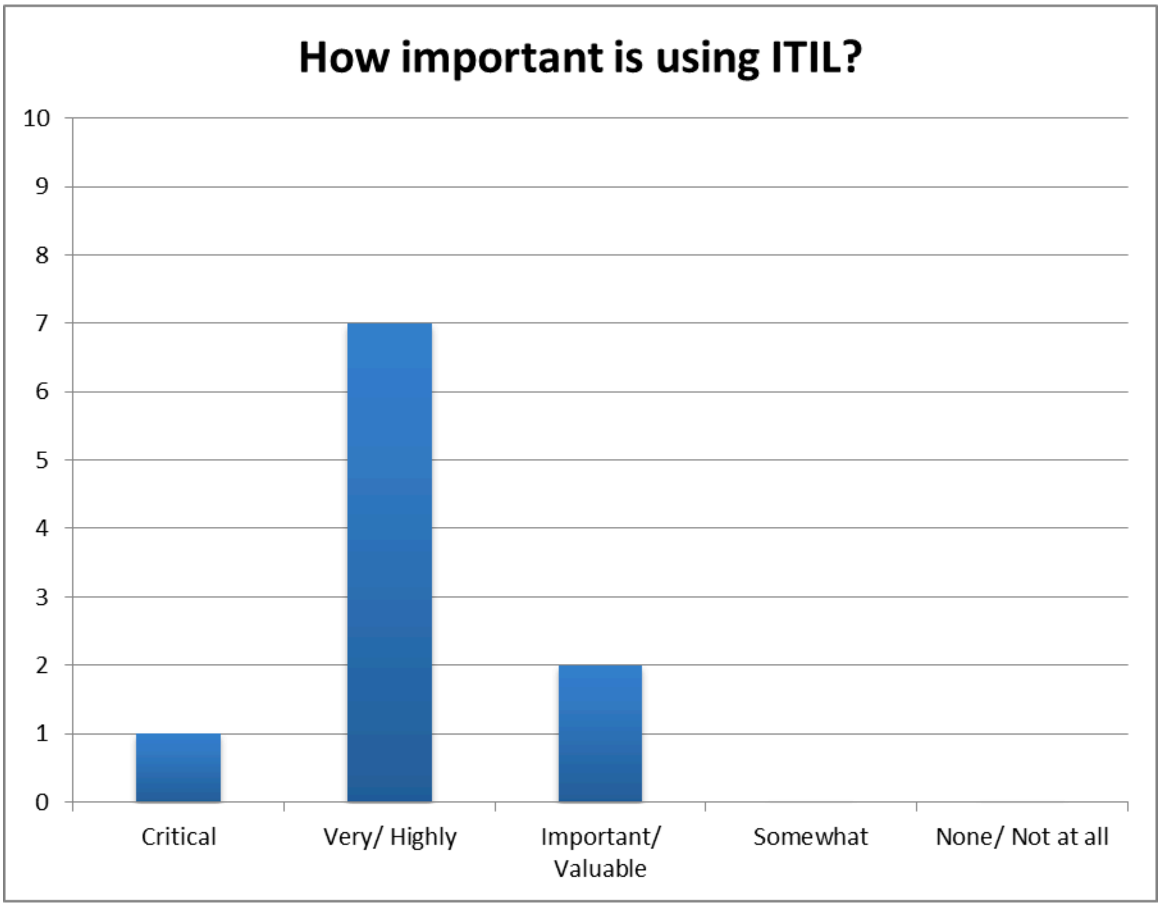


**Diagram ar – Response to question D-D**

Question: How important is each of the following to practising sound IT governance in your organisation? Using ITIL as the underlying practice for structuring IT services, their support and delivery.

Classification: Accepted

Deduction: Utilising ITIL is significantly important to practising sound IT governance.

Cross-reference: Recommendation 6

### Question D-E

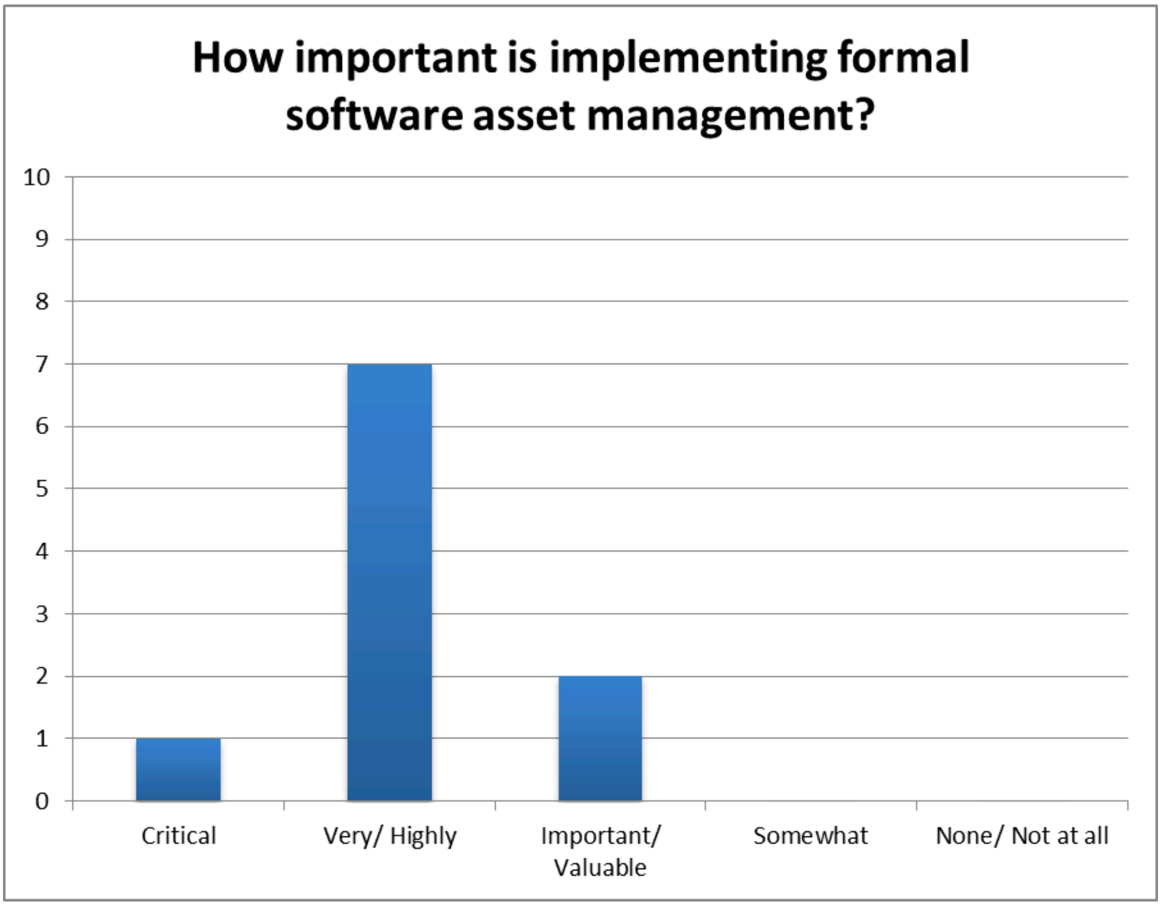


**Diagram as – Response to question D-E**

Question: How important is each of the following to practising sound IT governance in your organisation? Implementing formal software asset management to manage the software lifecycle.

Classification: Accepted

Deduction: Implementig formal software asset management is of importance to practising sound IT governance.

Cross-reference: Recommendation 14

## E. Risk management

### Question E-A

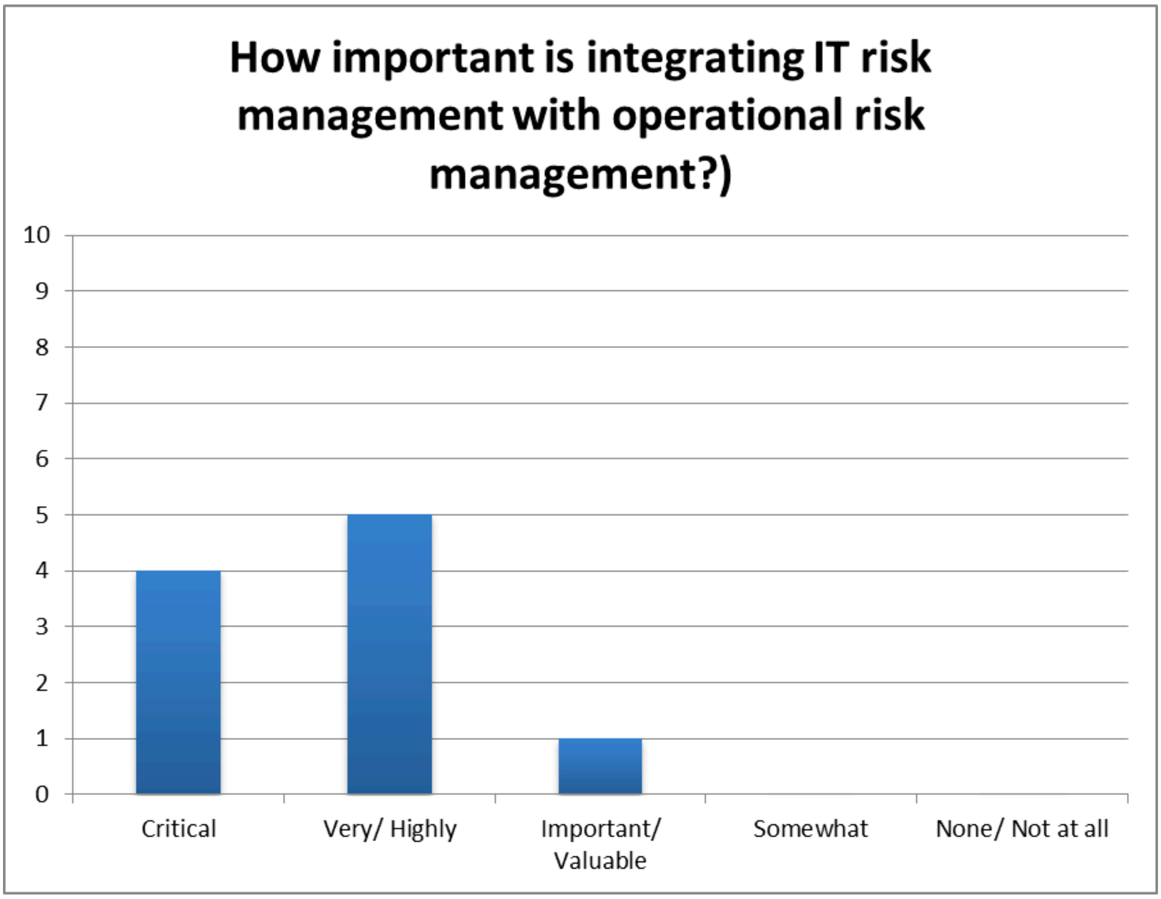


**Diagram at – Response to question E-A**

Question: How important is each of the following to sound IT risk management in your organisation? Integrating IT risk management with the operational risk management component of enterprise risk management (ERM).

Classification: Accepted

Deduction: Integrating IT risk management and operational risk management is significantly important to sound IT risk management.

Cross-reference: Recommendation 4

### Question E-B

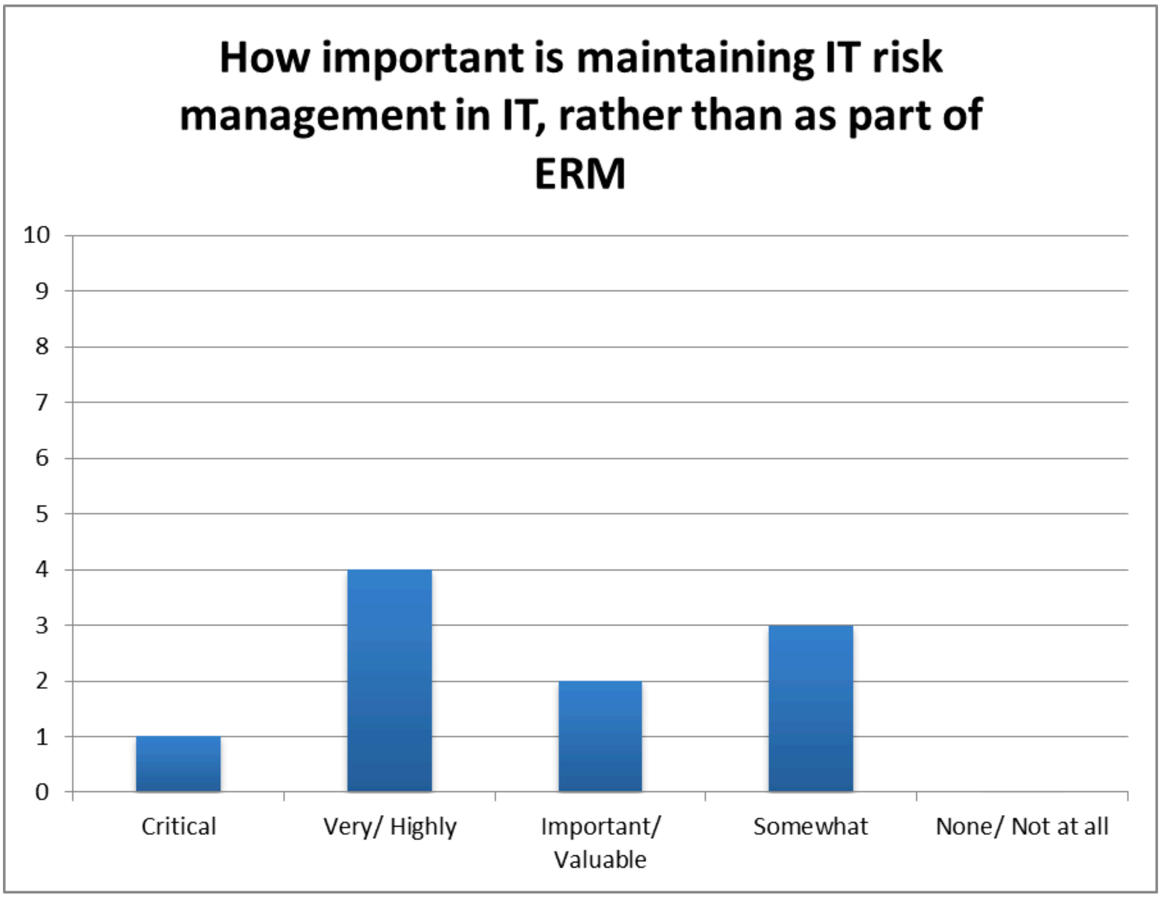


**Diagram au – Response to question E-B**

Question: How important is each of the following to sound IT risk management in your organisation? Maintaining an IT risk management function in IT, rather than having it as part of ERM.

Classification: Accepted

Deduction: This almost contradicts the preceding question, although the two questions could also be interpreted as that and ERM representative inside IT should be responsible for management of IT risk, as part of ERM.

Cross-reference: Recommendation 4

### Question E-C

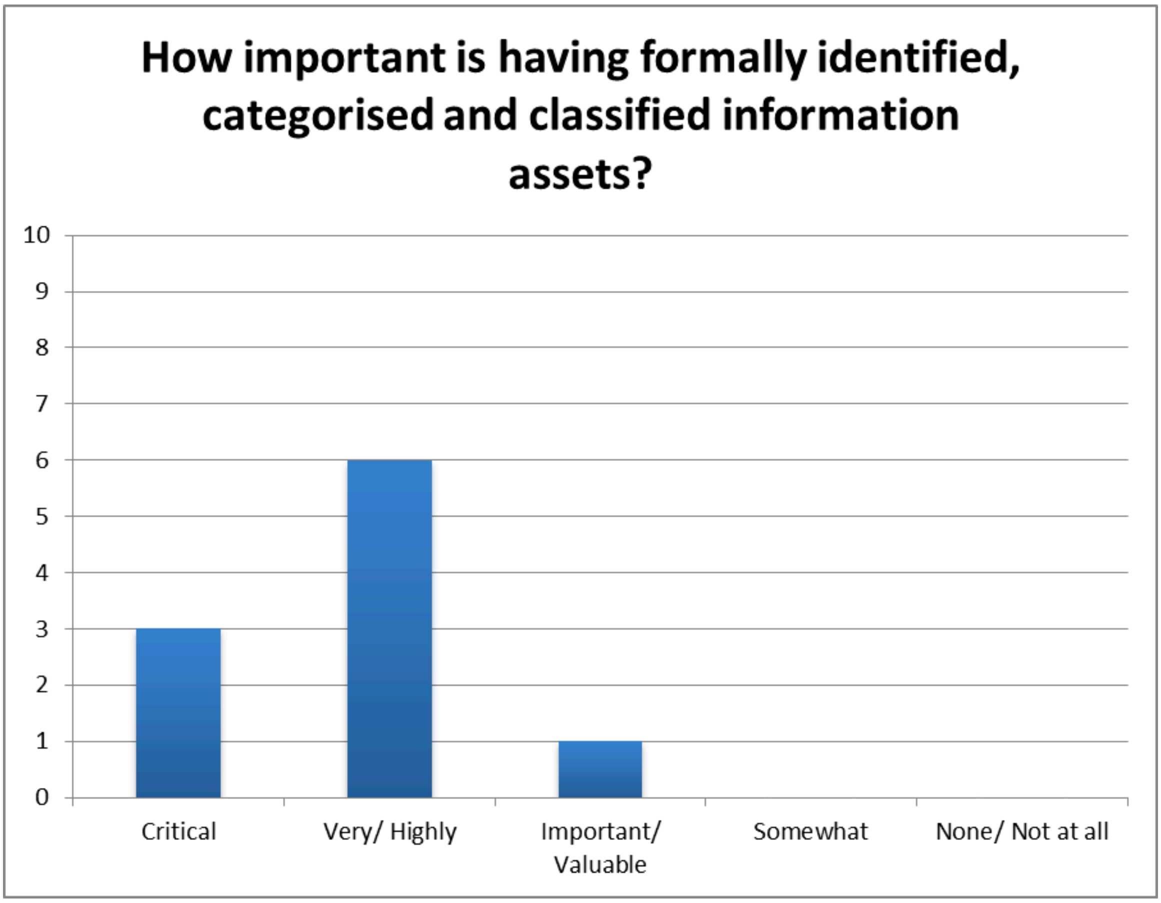


**Diagram av – Response to question E-C**

Question: How important is each of the following to sound IT risk management in your organisation? Having formally identified, categorised and classified information assets.

Classification: Accepted

Deduction: Having formally identified, categorised and classified information assets is of significant importance.

Cross-reference: Recommendation 13

### Question E-D

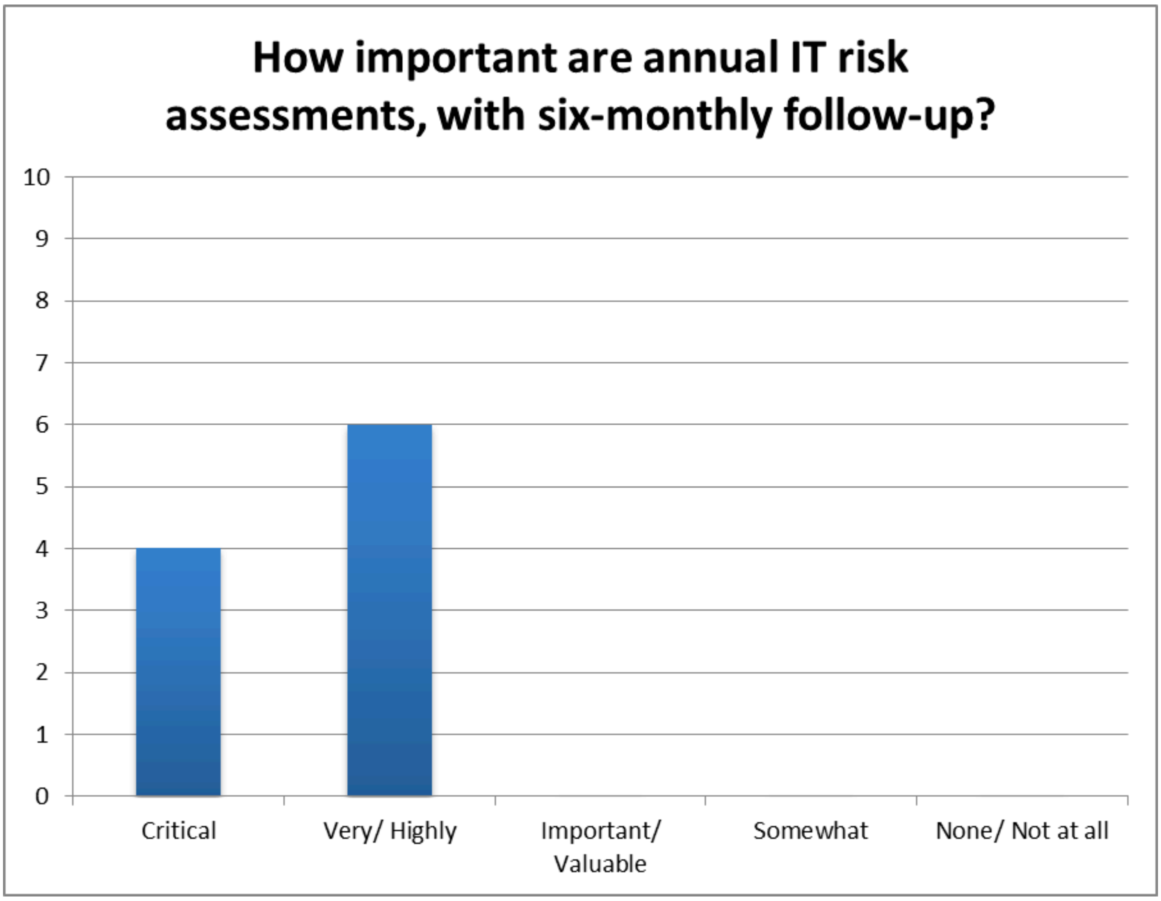


**Diagram aw – Response to question E-D**

Question: How important is each of the following to sound IT risk management in your organisation? Performing annual IT risk assessments, with six-monthly follow-up.

Classification: Accepted

Deduction: Performing annual IT risk assessments, with six-monthly follow-up is of significant importance.

Cross-reference: Recommendation 13

### Question E-E

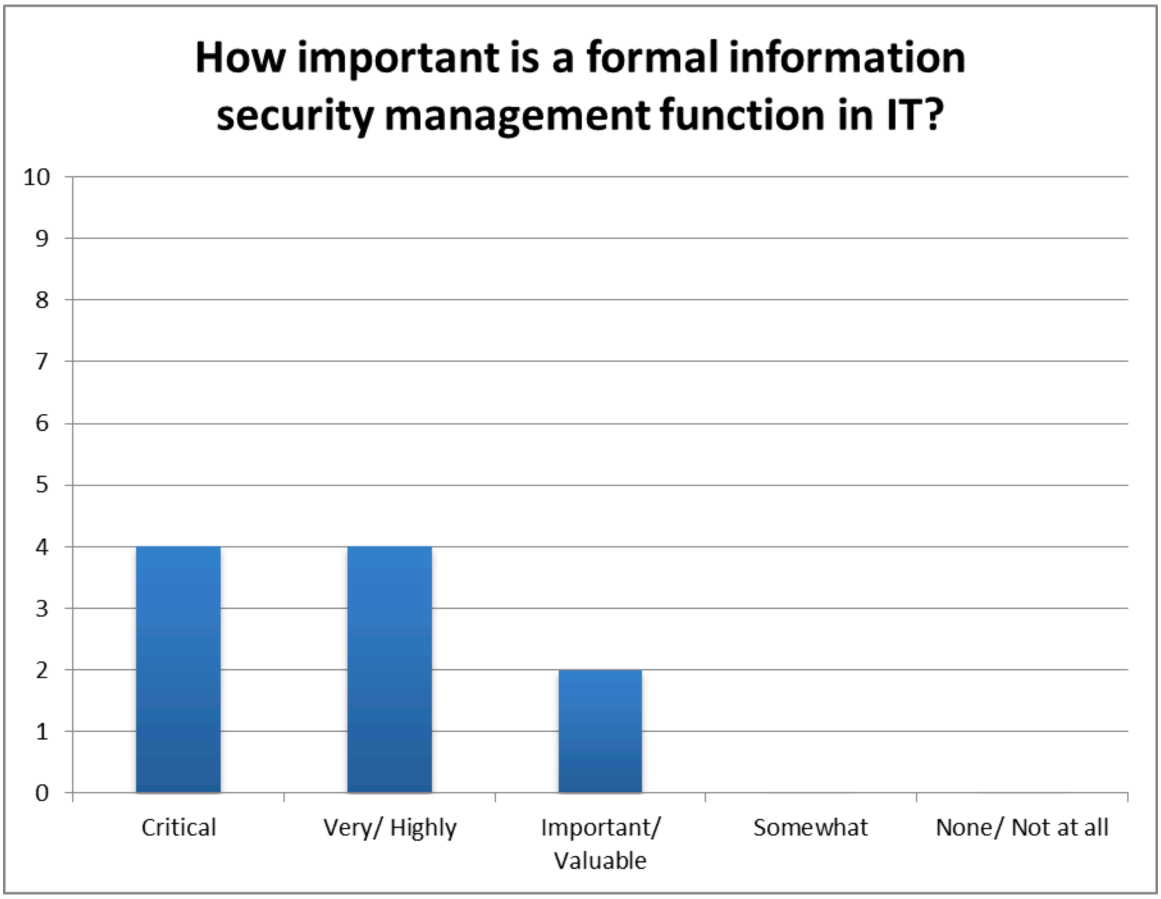


**Diagram ax – Response to question E-E**

Question: How important is each of the following to sound IT risk management in your organisation? Having a formal information security management function in IT?

Classification: Accepted

Deduction: Having a formal information security management function is of significant importance.

Cross-reference: Recommendations 6, 8

### Question E-F

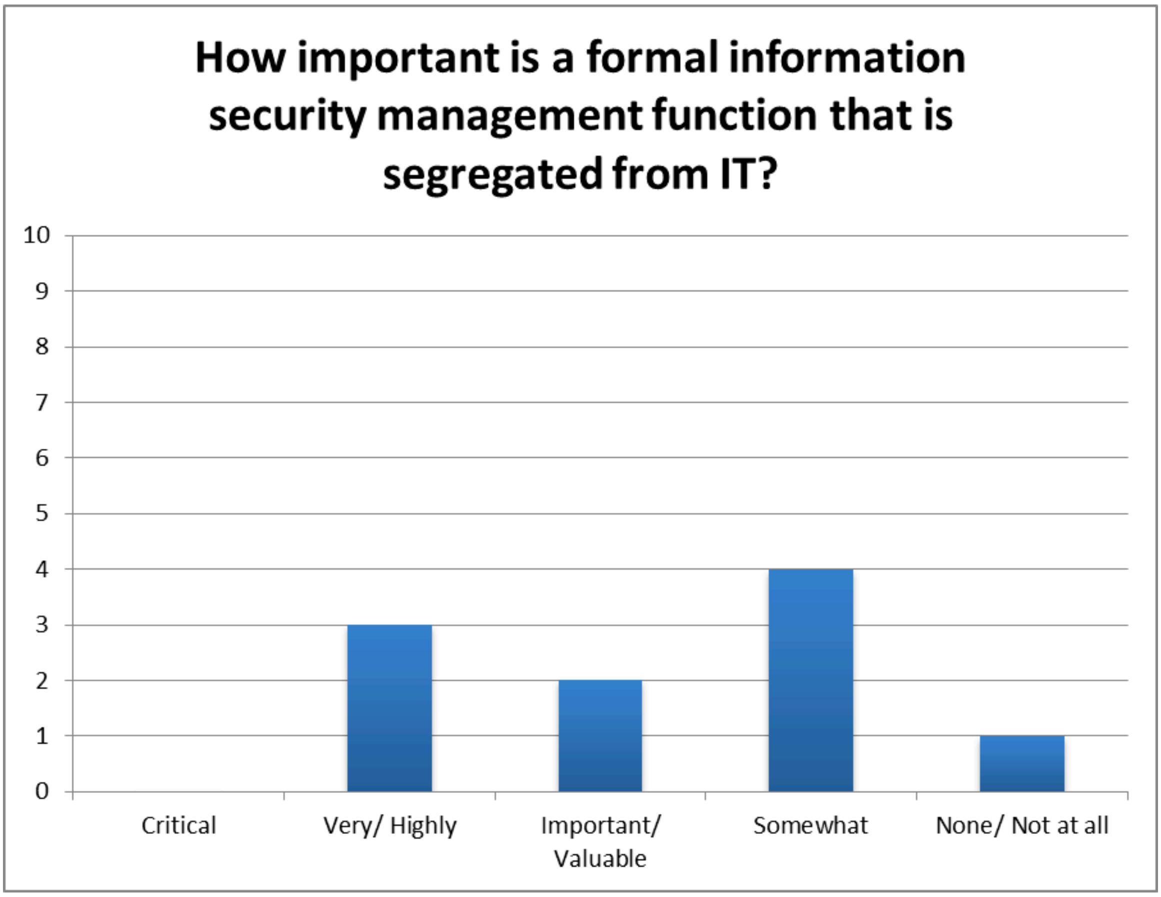


**Diagram ay – Response to question E-F**

Question: How important is each of the following to sound IT risk management in your organisation? Having a formal information security management function that is segregated from IT, i.e. as a business function.

Classification: Accepted

Deduction: Having a formal information security function that is segregated from IT is of significant importance.

Cross-reference: Recommendations 6, 8

### Question E-G

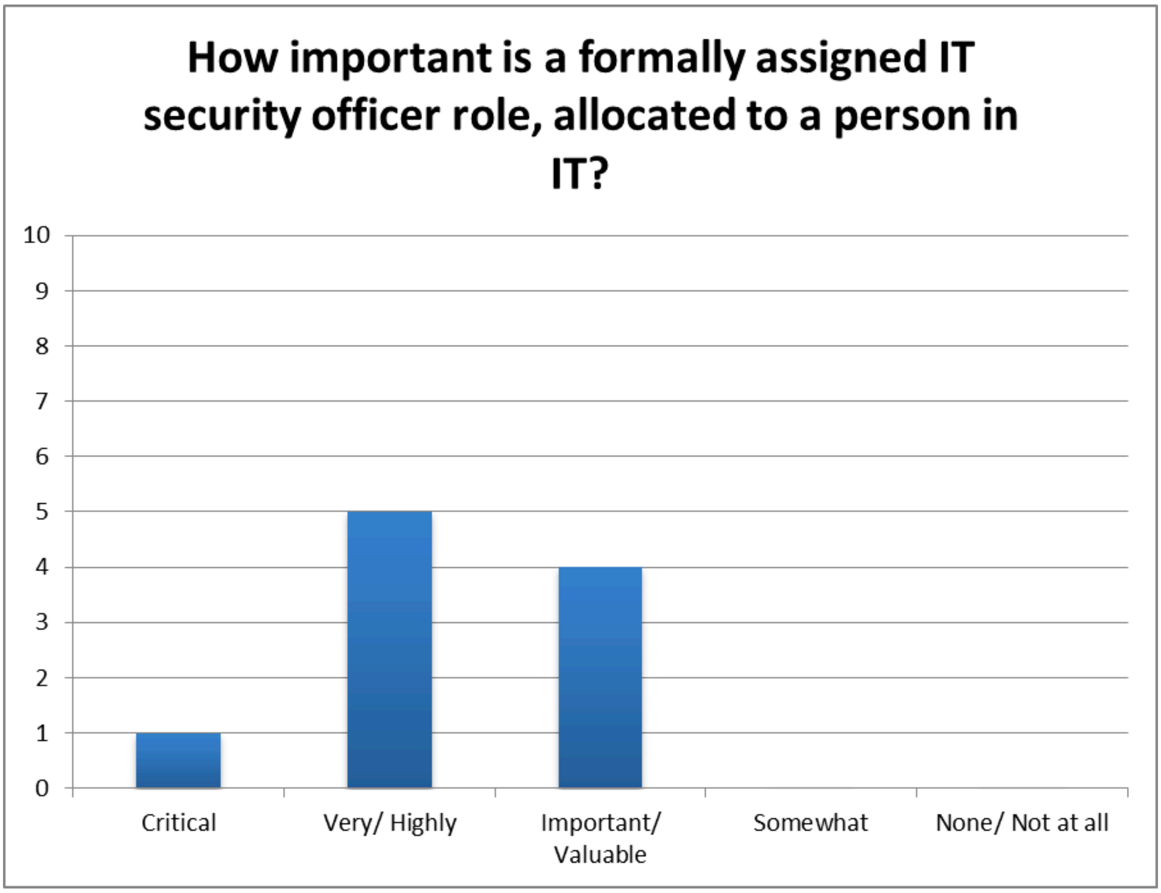


**Diagram az – Response to question E-G**

Question: How important is each of the following to sound IT risk management in your organisation? Having a formally assigned IT security officer role, allocated to a person in IT.

Classification: Accepted

Deduction: The information security role is important but it does not detract from the effectiveness of the role if it is situated inside the IT organisation. Although the preferred practice would be to locate this role outside IT, the preferred and practicable approach in South Africa is usually to locate this role in IT.

Cross-reference: Recommendation 23

### Question E-H

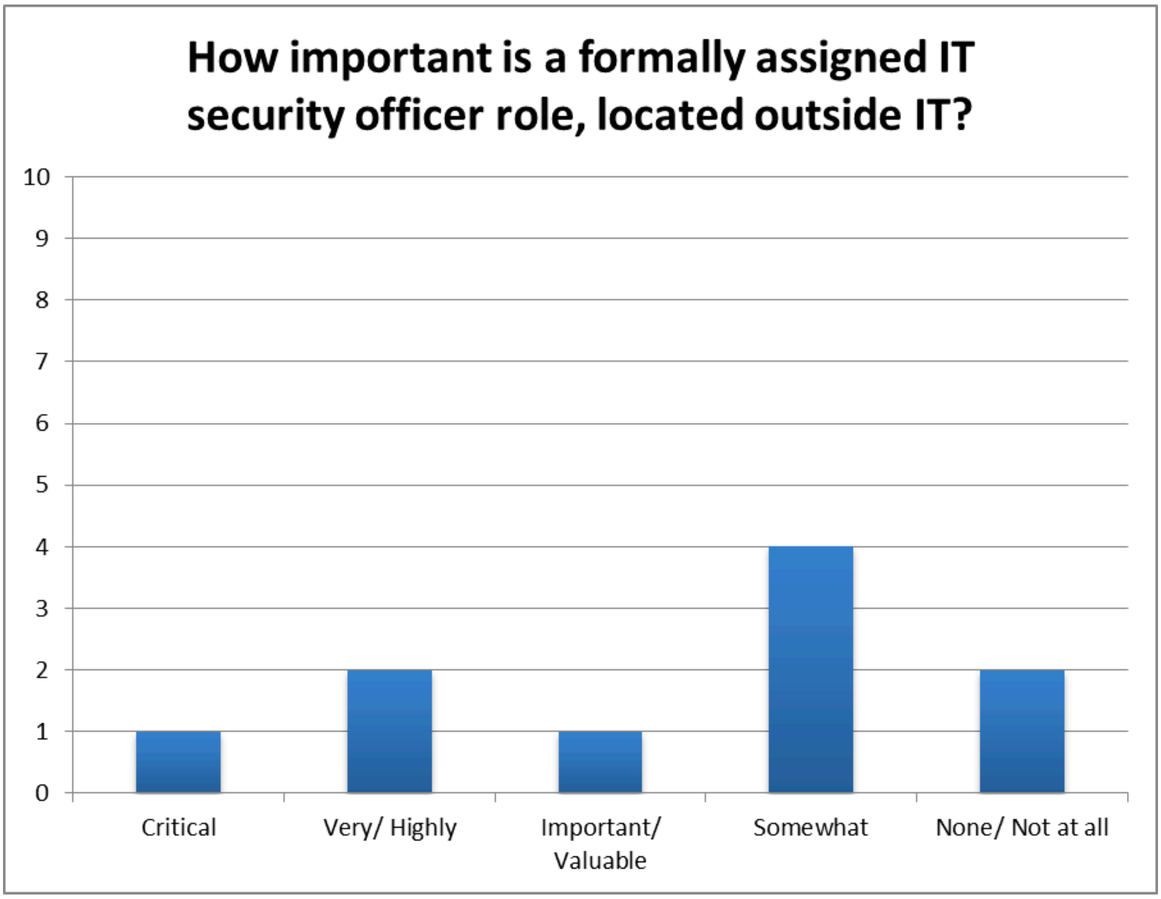


**Diagram ba – Response to question E-H**

Question: How important is each of the following to sound IT risk management in your organisation? Having a formally assigned IT security officer role, allocated to a person outside IT.

Classification: Not accepted

Deduction: The information security role is important, but it does not detract from the effectiveness of the role if it is situated inside the IT organisation. Although the preferred practice would be to locate this role outside IT, the preferred and practicable apporach in South Africa is usually to locate this role in IT.

Cross-reference: Recommendation 23

### Question E-I

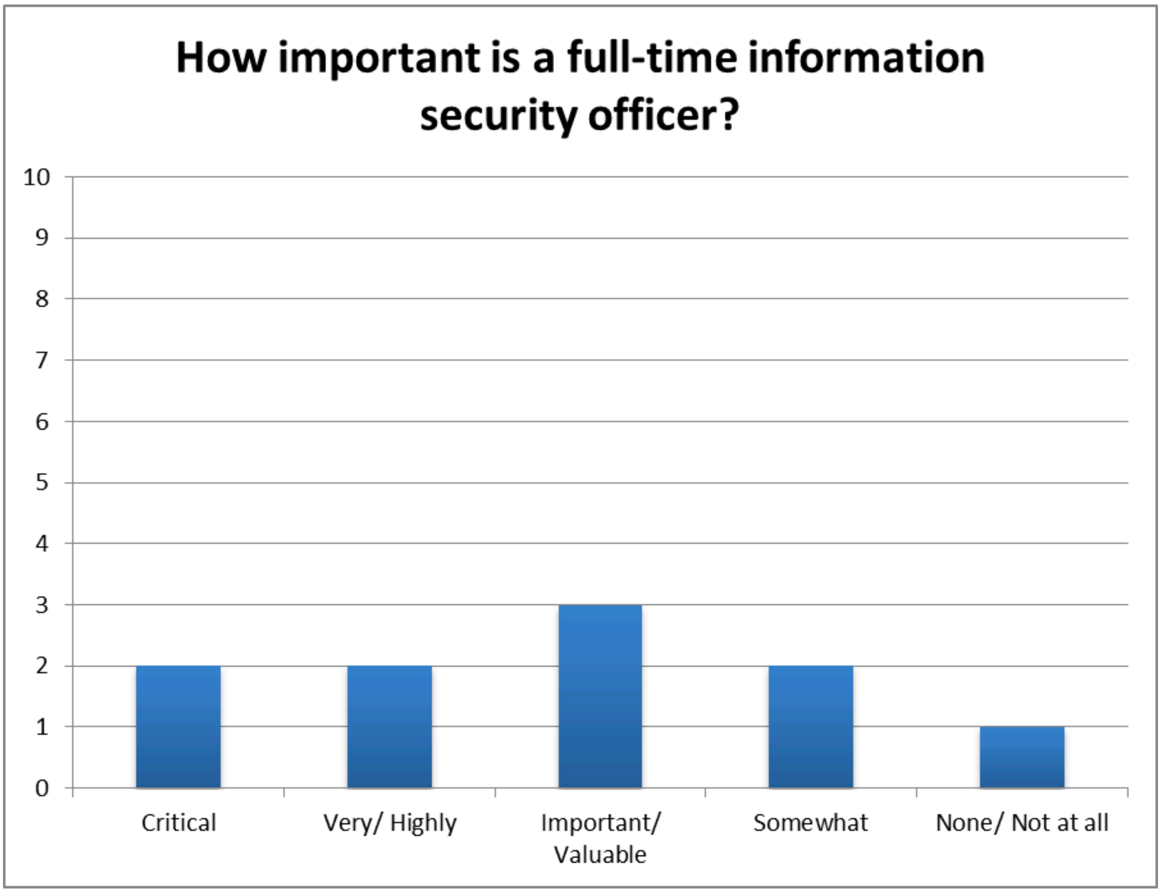


**Diagram bb – Response to question E-I**

Question: How important is each of the following to sound IT risk management in your organisation? Having a full-time information security officer.

Classification: Considered

Deduction: It is not significantly important to have a full-time information security officer.

Cross-reference: Recommendation 23

### Question E-J

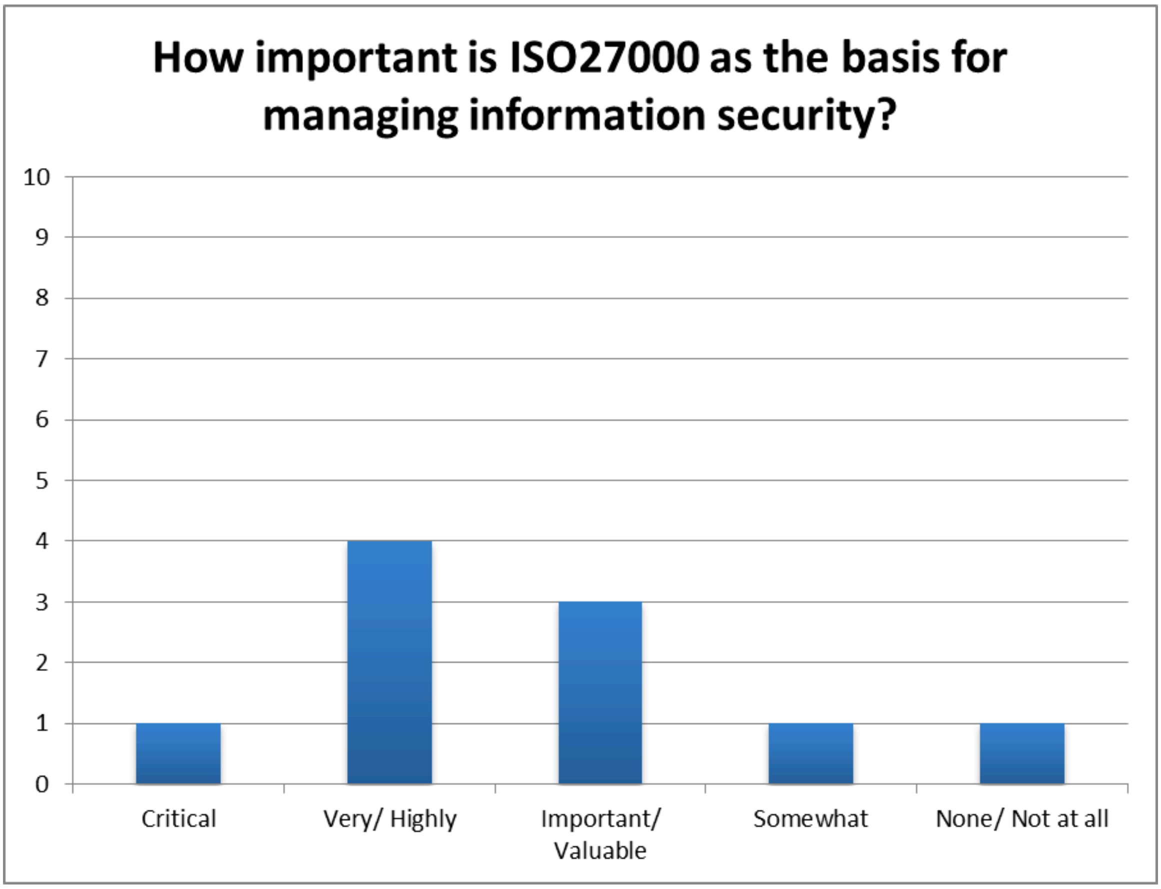


**Diagram bc – Response to question E-J**

Question: How important is each of the following to sound IT risk management in your organisation? Using ISO/IEC27000 as the basis for managing information security.

Classification: Accepted

Deduction: It is of imprtance to base information security management on ISO/IEC27000.

Cross-reference: Recommendation 8

## Question E-K

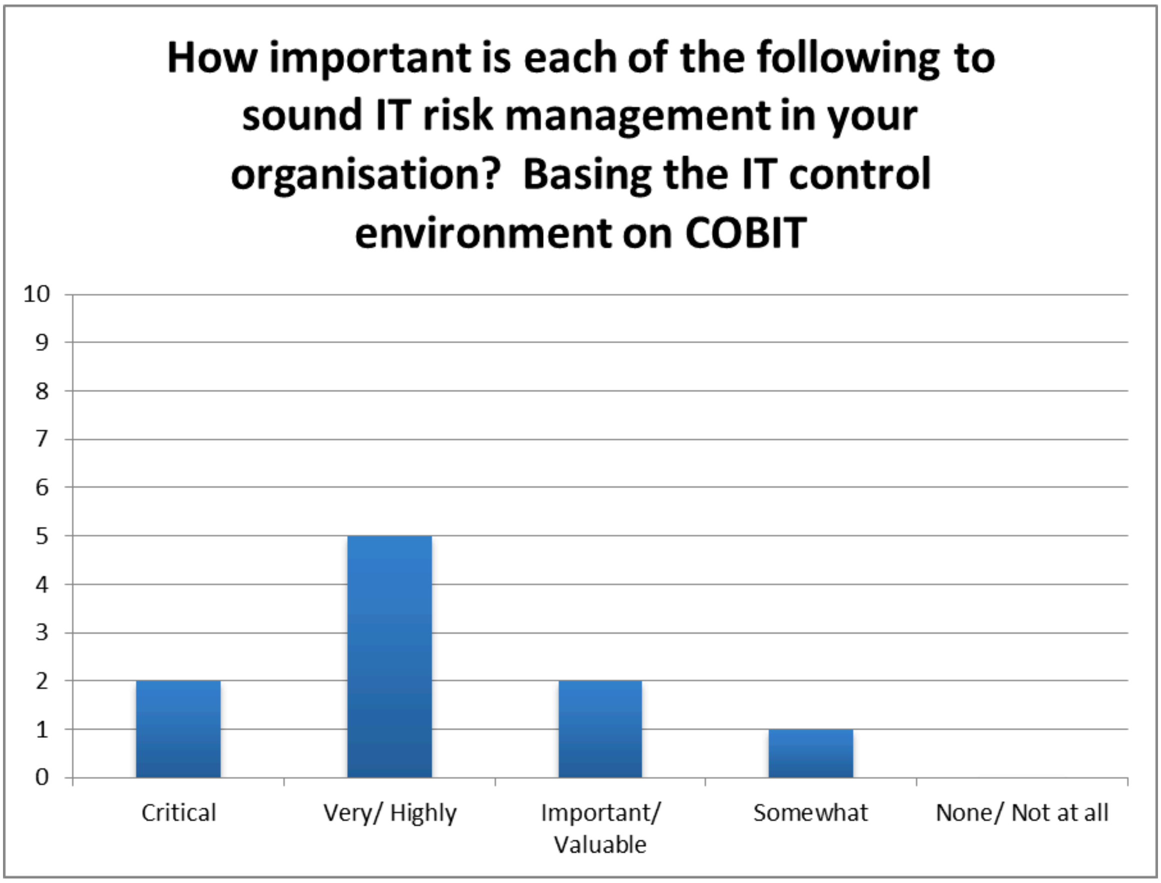


**Diagram bd – Response to question E-K**

Question: How important is each of the following to sound IT risk management in your organisation? Basing the IT control environment on COBIT.

Classification: Accepted

Deduction: Basing the IT control environment on COBIT is important.

Cross-reference: Recommendation 7

### Question E-L

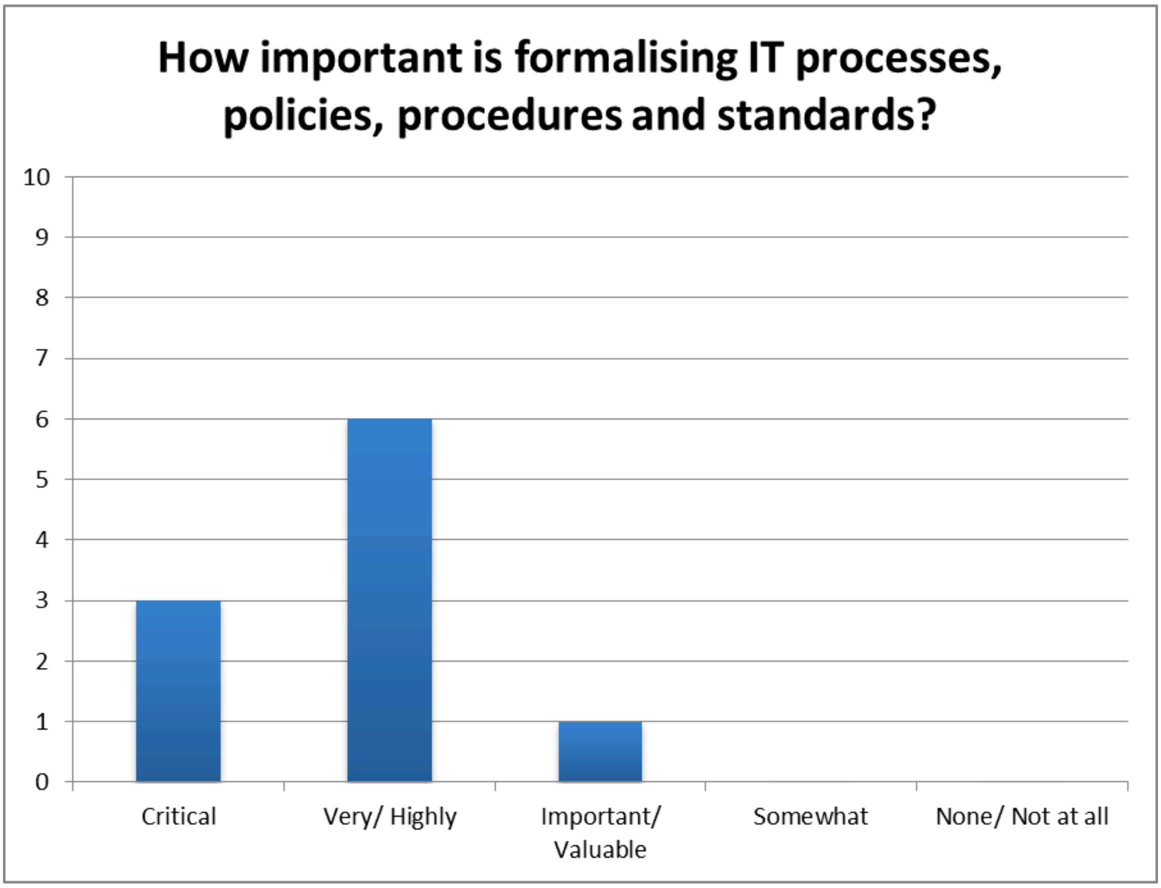


**Diagram be – Response to question E-L**

Question: How important is each of the following to sound IT risk management in your organisation? Formalising IT processes, policies, procedures and standards.

Classification: Accepted

Deduction: It is of significant importance to formalise IT processes, policies, procedures and standards.

Cross-reference: Recommendations 13, 15, 17

### Question E-M

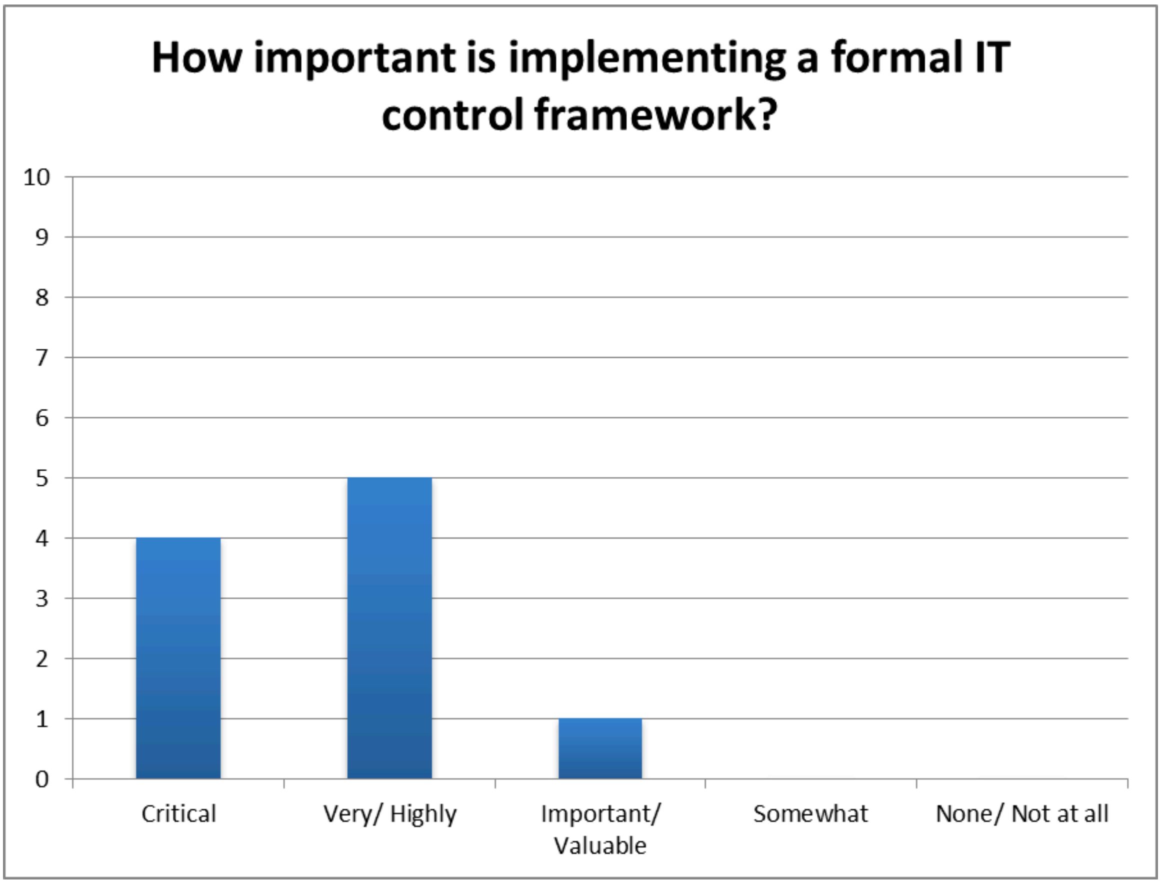


**Diagram bf – Response to question E-M**

Question: How important is each of the following to sound IT risk management in your organisation? Implementing a formal IT control framework.

Classification: Accepted

Deduction: It is significantly important to implement a formal IT control framework.

Cross-reference: Recommendation 16

### Question E-N

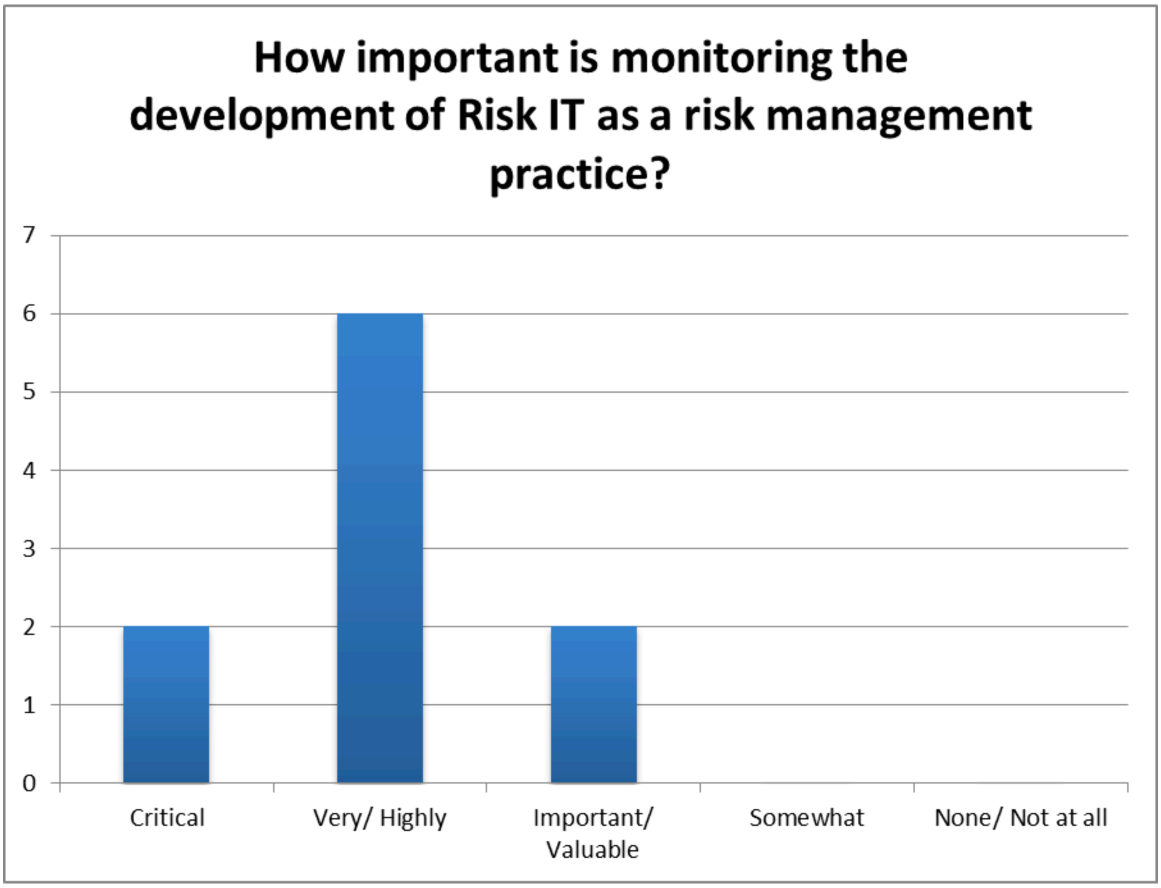


**Diagram bg – Response to question E-N**

Question: How important is each of the following to sound IT risk management in your organisation? Monitoring the development of Risk IT as a risk management practice, in order to consider its adoption once it has matured sufficiently

Classification: Accepted

Deduction: Monitoring the development of Risk IT is of significant importance.

Cross-reference: Recommendations 4, 7

## F. Performance measurement

### Questions F-A to F-B

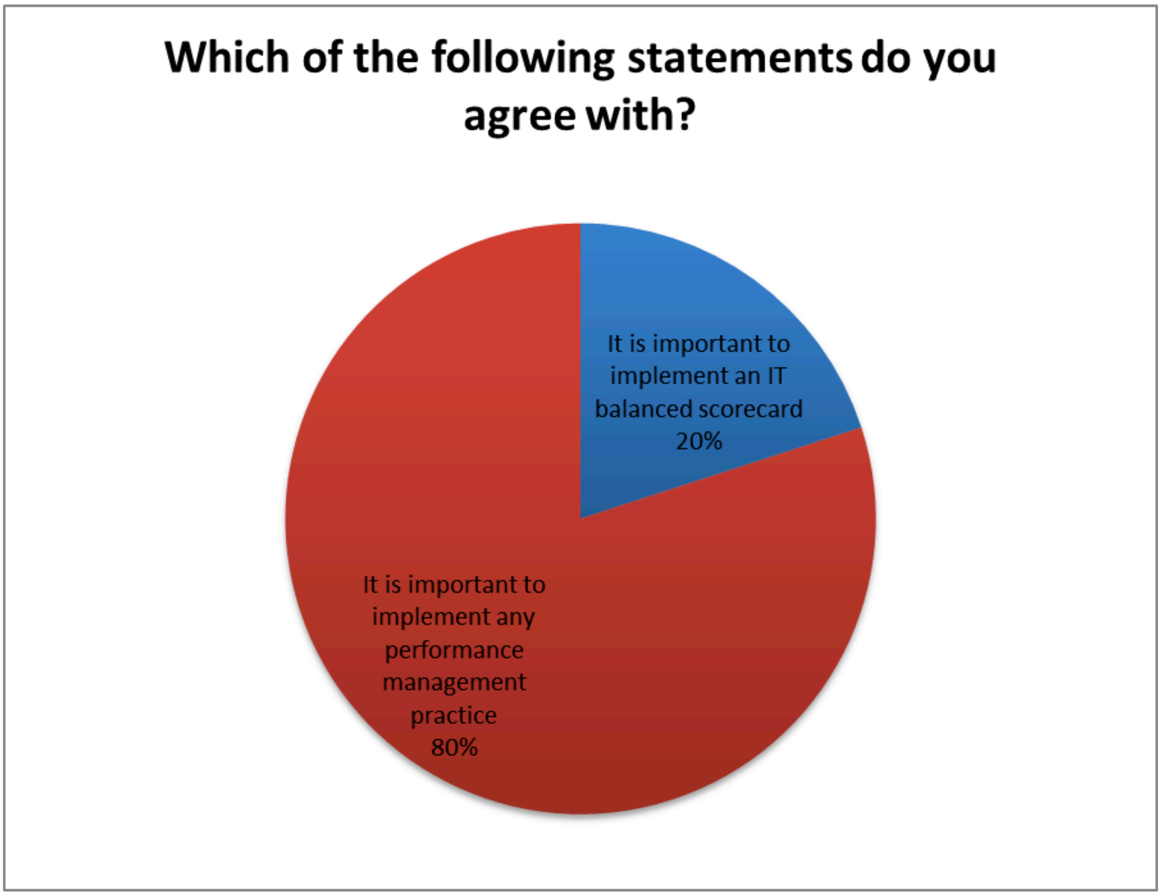


**Diagram bh – Response to questions F-A to B**

Question: Which of the following statements do you agree with? Please tick one.

Classification: Accepted F-A.2 – It is important to implement any performance management practice.

Deduction: IT performance management is important, regardless of whether a balanced scorecard is implemented or not.

Cross-reference: Recommendation 5, 9

# Appendix Three – Participant Input Data

| | | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **A. GENERAL** | | | | | | | | | | | | |
| A | How important is the Office of the CIO concept to you? | 3 | 3 | 4 | 0 | 0 | | 10 | Accepted | | | All respondents agreed that there is value in the Office of the CIO. | 21 |
| B | How important is the inclusion of operational roles below that of CIO in the framework? | 3 | 6 | 0 | 1 | 0 | | 10 | Accepted | | | The effectiveness of the Office of the CIO depends on the clarity of roles | 20 - 29 |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  |  |  |  |  |  |  |  |  |  |  |  | making up the Office. |  |
| C | How important is the role of an IT financial manager? | 4 | 3 | 0 | 2 | 1 |  | 10 | Accepted |  |  | The IT financial manager role is of significant importance and warrants a full-time appointment. | 25 |
| c.1 | Should the IT financial manager role be permanent or merely an allocated responsibility? Please tick one. |  |  |  |  |  |  |  |  |  |  |  |  |
| c.1.1 | Permanent |  |  |  |  |  | 6 | 10 |  | Accepted |  |  |  |
| c.1.2 | Allocated |  |  |  |  |  | 4 |  |  |  |  |  |  |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D | How important is the role of an IT risk officer? | 4 | 6 | 0 | 0 | 0 |  | 10 | Accepted |  |  | The IT risk officer role is of significant importance and warrants a full-time appointment. | 26 |
| d.1 | Should the IT risk officer role be permanent or merely an allocated responsibility? |  |  |  |  |  |  |  |  |  |  |  |  |
| d.1.1 | Permanent |  |  |  |  |  | 7 | 10 |  | Accepted |  |  |  |
| d.1.2 | Allocated |  |  |  |  |  | 3 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | How important is the role of the: |  |  |  |  |  |  |  |  |  |  |  |  |
| E | Applications manager? | 4 | 4 | 2 | 0 | 0 |  | 10 | Accepted |  |  | The role is of significant importance. | 27 |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| F | Technical manager? | 2 | 6 | 2 | 0 | 0 |  | 10 | Accepted |  |  | The role is of significant importance. | 28 |
| G | IT operations manager? | 6 | 1 | 2 | 1 | 0 |  | 10 | Accepted |  |  | The role is of critical importance. | 29 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| H | How important is it to segregate IT operations and technical manager roles? | 1 | 2 | 3 | 3 | 1 |  | 10 | Considered |  |  | The technical manager role could be combined with other roles without compromising its effectiveness. | 28 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| I | Who should be responsible for IT service support? Please tick one. |  |  |  |  |  |  | 13 |  |  |  | A dedicated service | 28 |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| i.1 | Applications manager |  |  |  |  |  | 2 |  |  |  | Not Accepted | support role is significantly important, with a preferred reporting line to the operations manager. |  |
| i.2 | Technical manager |  |  |  |  |  | 2 |  |  |  | Not Accepted |  |  |
| i.3 | Operations manager |  |  |  |  |  | 3 |  |  |  | Not Accepted |  |  |
| i.4 | A dedicated IT service support manager reporting to the technical manager role |  |  |  |  |  | 0 |  |  |  | Not Accepted |  |  |
| i.5 | A dedicated IT service support manager reporting to the operations manager |  |  |  |  |  | 6 |  |  |  | Accepted |  |  |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| j | Who should be responsible for IT service delivery? Please tick one. |  |  |  |  |  |  | 12 |  |  |  | Two participants selected two options, namely j.3 and j.5. |  |
| j.1 | Applications manager |  |  |  |  |  | 1 |  |  |  | Not Accepted |  |  |
| j.2 | Technical manager |  |  |  |  |  | 0 |  |  |  | Not Accepted |  |  |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| j.3 | Operations manager |  |  |  |  |  | 4 |  |  |  | Not Accepted | A dedicated service delivery role is important, which could be assigned to the IT operations manager. As there is no consensus as to which option is preferable, both j.3 and j.5 will be accommodated in the framework. | 29 |
| j.4 | A dedicated IT service delivery manager reporting to the technical manager role |  |  |  |  |  | 2 |  |  |  | Not Accepted |  |  |

| | | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| j.5 | A dedicated IT service delivery manager reporting to the operations manager role | | | | | | 5 | | | | Considered | A dedicated service delivery position is important, with a preferred reporting line to the operations manager. | 29 |
| | | | | | | | | | | | | | |
| K | Do you believe an IT governance framework should be prescriptive on whether a centralised, federated or hybrid IT organisational model should be adopted? Please tick “yes” or “no”. | | | | | | | 10 | | | | | |
| k.1 | Yes | | | | | | 5 | | | Undecided | | The IT operational model depends on and should follow the culture of the organisation.  This is the conclusion, | In the interest of deriving a generic framework, the researche decided not to include a prescriptive |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  |  |  |  |  |  |  |  |  |  |  |  | based on the divided opinion to this criterion. | recommendation on IT organisational structure. |
| k.2 | No |  |  |  |  |  | 5 |  |  |  |  |  |  |
| 1 | How important is vendor management to an IT governance framework? | 1 | 8 | 1 | 0 | 0 |  | 10 | Accepted |  |  | Vendor management is significantly important to the framework. | 3, 13, 14, 21, 31 |
| M | Which of the following options do you prefer for IT procurement? Please tick one |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| m.1 | IT procurement should be a normal part of the corporate procurement process |  |  |  |  |  | 6 | 10 |  | Accepted |  | It is preferred that IT procurement is a normal part of the corporate procurement process. | 13, 21, 25 |
| m.2 | IT procurement should be a process independent of the corporate procurement process |  |  |  |  |  | 4 |  |  |  |  | Some organisations have a more federal structure, which allows support functions like IT to embed procurement into its operations. As four out of ten participants preferred this | Not included |

| | | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | approach, it would be mentioned as an option in the framework. | |
| N | Which of the following options do you prefer (please tick one) for IT vendor management? | | | | | | | 10 | | | | | |
| n.1 | IT procurement should be a normal part of the corporate procurement process but IT vendor management should be separate from the corporate function | | | | | | 5 | | | Undecided | | Depending on the organisation, the Procurement | 13, 25 |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| n.2 | IT procurement and IT vendor management should be separate from the corporate function and procurement processes |  |  |  |  |  | 5 |  |  |  |  | function might handle all aspects of IT procurement and IT vendor management. This is the deduction, based on the split opinion of participants. |  |
| O | How important is the role of an IT Steering Committee in your organisation? | 4 | 4 | 2 | 0 | 0 |  | 10 | Accepted |  |  | An IT Steering Committee is significantly important. | 31 |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| P | How important is the role of an IT Strategy Committee in your organisation? | 2 | 3 | 3 | 1 | 1 |  | 10 | Accepted |  |  | An IT Strategy Committee is significantly important, yet non-structured input by participants an q.2 below suggested that there is a preference to combine the IT Strategy Committee and IT Steering Committee. | 30 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Q | Would you prefer to have separate IT strategy and Steering Committees or combine them?  Please tick one. |  |  |  |  |  |  | 10 |  |  |  |  |  |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| q.1 | Separate |  |  |  |  |  | 2 |  |  |  |  |  |  |
| q.2 | Combined |  |  |  |  |  | 8 |  |  | Accepted |  | The preferred approach is to combine the IT strategy role with that of the IT Steering Committee. | 30, 31 |
| R | How important is it to have a formal chief technology officer role? | 0 | 3 | 2 | 3 | 2 |  | 10 | Considered |  |  | The CTO role is useful, but not of high importance. | 21, 22 |
| S | How important is it to segregate the chief technology officer role from that of the CIO and other IT roles? | 0 | 3 | 2 | 3 | 2 |  | 10 | Considered |  |  | IT is not highly important to segregate the CIO and CTO roles. |  |

| | | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | |
| | ***Practices*** | | | | | | | | | | | | |
| t | How important is implementing the IT governance chapter of the King III Code of Corporate Governance to your IT governance objectives? | 4 | 5 | 1 | 0 | 0 | | 10 | Accepted | | | It is of significant importance to implement Chapter 5 of King III | 13 |
| U | How important is implementing the concepts of the ISO/IEC38500 IT governance standard to your IT governance objectives? | 0 | 2 | 5 | 3 | 0 | | 10 | Considered | | | It is not highly important to implement ISO/IEC38500. | 14 |
| | | 38 | 59 | 29 | 17 | 7 | ***150*** | | | | | | |
| | **B. STRATEGIC ALIGNMENT** | | | | | | | | | | | | |
| | ***IT Goals and Objectives*** | | | | | | | | | | | | |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  | How often **<u>should you</u>** revisit your IT strategy and re-align it to the corporate strategy? Please tick one. |  |  |  |  |  |  |  |  |  |  |  |  |
| a | Annually |  |  |  |  |  | 3 | 10 |  |  | Not Accepted | IT strategy should be updated at least annually, with consideration to be given to an update midway through the year. There was consensus that an update should take place at least annually, but some participants felt that updates should | 1 |
| B | Annually, with an update halfway through the year |  |  |  |  |  | 3 |  |  |  | Not Accepted |  |  |
| c | Every third year |  |  |  |  |  | 1 |  |  |  | Not Accepted |  |  |
| d | Every third year, with annual updates |  |  |  |  |  | 1 |  |  |  | Not Accepted |  |  |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| e | A different frequency from the above – please specify. |  |  |  |  |  | 2 |  |  |  | Not Accepted | make whenever business change requires that, even if at irregular intervals throughout the year. |  |
|  | ***Enterprise architecture*** |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Which of the following statements do you agree with? Please tick each option you agree with. |  |  |  |  |  |  |  |  |  |  |  |  |
| F | Enterprise architecture is a business rather than IT function |  |  |  |  |  | 4 |  |  |  | Not Accepted |  |  |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| g | The business architecture belongs to business, the remaining architecture layers belong to the IT function |  |  |  |  |  | 6 |  |  |  | Accepted | The business architecture belongs to business, the remaining architecture layers belong to the IT function. | 1, 18, 24 |
| H | Enterprise architecture should be closely linked to the corporate strategy function, to translate strategy to action |  |  |  |  |  | 8 |  |  |  | Accepted | Enterprise architecture should be closely linked to the corporate strategy function, to translate strategy to action. | 18, 32 |
| I | It is important to have a dedicated enterprise architect |  |  |  |  |  | 6 |  |  |  | Accepted | Despite indications that a dedicated | 24 |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  |  |  |  |  |  |  |  |  |  |  |  | enterprise architect role is required, non-structured input indicated that the IT architect role should be emphasized instead. |  |
| J | It is important to have an Enterprise Architecture Forum |  |  |  |  |  | 5 |  |  |  | Considered | Based on non-structured input, it was decided to rather emphasise the importance of a technology architecture forum. | 1, 11, 24, 32 |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K | It is important to align IT services to the IT strategy on an ongoing basis |  |  |  |  |  | 9 |  |  |  | Accepted | It is important to align IT services to the IT strategy on an ongoing basis. | 1, 19 |
|  | ***Practices*** |  |  |  |  |  |  |  |  |  |  |  |  |
|  | How important is each of the following to sound IT governance? |  |  |  |  |  |  |  |  |  |  |  |  |
| L | Following TOGAF as a desirable practice | 0 | 0 | 6 | 2 | 2 |  | 10 | Considered |  |  | Practice accepted, although non-structured input indicated that the adoption of architecture practices is more important than | 11 |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | **Deduction** | **Cross-reference to Recommendations** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  |  |  |  |  |  |  |  |  |  |  |  | adopting TOGAF as such. |  |
| M | Following an enterprise architecture methodology, regardless of the adopted practice | 0 | 3 | 6 | 1 | 0 |  | 10 | Considered |  |  | Practice accepted. | 11 |
| N | Integration between enterprise architecture and corporate strategy | 5 | 2 | 3 | 0 | 0 |  | 10 | Accepted |  |  | Practice accepted. | 32 |
|  |  | 5 | 5 | 15 | 3 | 2 | ***30*** |  |  |  |  |  |  |
|  | **C. VALUE DELIVERY** |  |  |  |  |  |  |  |  |  |  |  |  |
|  | How important is each of the following to sound value delivery in your organisation? |  |  |  |  |  |  |  |  |  |  |  |  |
| A | Having an enterprise PMO that also handles IT projects | 1 | 5 | 1 | 1 | 2 |  | 10 | Accepted |  |  | Practice accepted. | 33 |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| B | Having an IT programme management office (PMO), regardless of whether an enterprise PMO exists or not | 0 | 7 | 3 | 0 | 0 |  | 10 | Accepted |  |  | Practice accepted. | 33 |
| C | Including IT portfolio management in enterprise portfolio management | 2 | 3 | 2 | 3 | 0 |  | 10 | Accepted |  |  | Practice accepted. | 19 |
| D | Practising IT portfolio management, regardless of whether enterprise portfolio management is practised or not | 3 | 7 | 0 | 0 | 0 |  | 10 | Accepted |  |  | Practice accepted. | 19 |
| E | Practising IT service portfolio management to ensure continual alignment of services to the organisational strategy | 1 | 8 | 1 | 0 | 0 |  | 10 | Accepted |  |  | Practice accepted. | 19 |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| F | Following the development of ValIT and implementing the framework once it has matured sufficiently | 0 | 2 | 6 | 2 | 0 |  | 10 | Considered |  |  | Practice accepted. | 2, 7, 19, 20 |
| G | Following a formal project management methdology | 6 | 3 | 1 | 0 | 0 |  | 10 | Accepted |  |  | Practice accepted. | 3, 10, 14, 34 |
| H | Practising formal service level management | 6 | 3 | 1 | 0 | 0 |  | 10 | Accepted |  |  | Practice accepted. | 2, 3 |
|  | ***Practices*** |  |  |  |  |  |  |  |  |  |  |  |  |
|  | How important is each of the following to sound IT governance in your organisation? |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| I | Following Prince2 as a project management method | 2 | 0 | 6 | 2 | 0 |  | 10 | Considered |  |  | Practice accepted. | 10 |
| J | Following PMBOK as the underlying project management philosophy, regardless of what other methodologies are used | 2 | 2 | 4 | 2 | 0 |  | 10 | Considered |  |  | Practice accepted. | 10 |
| K | Having any formal project management methodology, regardless of whether it is Prince2 or another | 1 | 7 | 2 | 0 | 0 |  | 10 | Accepted |  |  | Practice accepted. | 10 |

| | | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| L | Monitoring the development of Val IT as a value management practice, in order to consider its adoption once it has matured sufficiently | 0 | 4 | 4 | 2 | 0 | | 10 | Considered | | | Practice accepted. | 2, 7, 19, 20 |
| | | 24 | 51 | 31 | 12 | 2 | ***120*** | | | | | | |
| | **D. RESOURCE MANAGEMENT** | | | | | | | | | | | | |
| | How important is each of the following to sound IT resource management in your organisation? | | | | | | | | | | | | |
| A | Adhering to corporate resource management processes, as part of IT governance | 2 | 4 | 4 | 0 | 0 | | 10 | Accepted | | | Practice accepted. | 3 |
| B | Implementing formal IT service support and service delivery processes | 3 | 7 | 0 | 0 | 0 | | 10 | Accepted | | | Practice accepted. | 6 |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C | Implementing a dedicated help desk or service desk to facilitate effective IT service management | 6 | 2 | 2 | 0 | 0 |  | 10 | Accepted |  |  | Practice accepted. | This aspect was toned down, as this is a more operational rather than governance consideration. ITIL is still recommended, which implies the implementation of a service desk. |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | ***Practices*** |  |  |  |  |  |  |  |  |  |  |  |  |
|  | How important is each of the following to sound IT governance in your organisation? |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D | Using ITIL as the underlying practice for structuring IT services, their support and delivery | 1 | 7 | 2 | 0 | 0 |  | 10 | Accepted |  |  | Practice accepted. | 6 |
| E | Implementing formal software asset management to manage the software lifecycle | 1 | 7 | 2 | 0 | 0 |  | 10 | Accepted |  |  | Practice accepted. | 14 |
|  |  | 13 | 27 | 10 | 0 | 0 | ***50*** |  |  |  |  |  |  |
|  | **E. RISK MANAGEMENT** |  |  |  |  |  |  |  |  |  |  |  |  |
|  | How important is each of the following to sound IT risk management in your organisation? |  |  |  |  |  |  |  |  |  |  |  |  |
| A | Integrating IT risk management with the operational risk management component of enterprise risk management (ERM) | 4 | 5 | 1 | 0 | 0 |  | 10 | Accepted |  |  | Practice accepted. | 4 |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| B | Maintaining an IT risk management function in IT, rather than having it as part of ERM | 1 | 4 | 2 | 3 | 0 |  | 10 | Accepted |  |  | Practice accepted. |  |
| C | Having formally identified, categorised and classified information assets | 3 | 6 | 1 | 0 | 0 |  | 10 | Accepted |  |  | Practice accepted. | 13 |
| D | Performing annual IT risk assessments, with six-monthly follow-up | 4 | 6 | 0 | 0 | 0 |  | 10 | Accepted |  |  | Practice accepted. | 13 |
| E | Having a formal information security management function in IT | 4 | 4 | 2 | 0 | 0 |  | 10 | Accepted |  |  | Practice accepted. | 6, 8 |
| F | Having a formal information security management function that is segregated from IT, i.e. as a business function | 0 | 3 | 2 | 4 | 1 |  | 10 | Considered |  |  | Practice accepted. |  |
| G | Having a formally assigned IT security officer role, allocated to a person in IT | 1 | 5 | 4 | 0 | 0 |  | 10 | Accepted |  |  | The information security role is | 23 |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| H | Having a formally assigned IT security officer role, allocated to a person outside IT | 1 | 2 | 1 | 4 | 2 |  | 10 | Not Accepted |  |  | important, but it does not detract from the effectiveness of the role if it is situated inside the IT organisation. |  |
| I | Having a full-time information security officer | 2 | 2 | 3 | 2 | 1 |  | 10 | Considered |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | ***Practices*** |  |  |  |  |  |  |  |  |  |  |  |  |
|  | How important is each of the following to sound IT governance in your organisation? |  |  |  |  |  |  |  |  |  |  |  |  |
| J | Using ISO/IEC27000 as the basis for managing information security | 1 | 4 | 3 | 1 | 1 |  | 10 | Accepted |  |  | Practice accepted. | 8 |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K | Basing the IT control environment on COBIT | 2 | 5 | 2 | 1 | 0 |  | 10 | Accepted |  |  | Practice accepted. | 7 |
| L | Formalising IT processes, policies, procedures and standards | 3 | 6 | 1 | 0 | 0 |  | 10 | Accepted |  |  | Practice accepted. | 13, 15, 17 |
| M | Implementing a formal IT control framework | 4 | 5 | 1 | 0 | 0 |  | 10 | Accepted |  |  | Practice accepted. | 16 |
| N | Monitoring the development of Risk IT as a risk management practice, in order to consider its adoption once it has matured sufficiently | 2 | 6 | 2 | 0 | 0 |  | 10 | Accepted |  |  | Practice accepted. | 4, 7 |
|  |  | 32 | 63 | 25 | 15 | 5 | ***140*** |  |  |  |  |  |  |
|  | **F. PERFORMANCE MEASUREMENT** |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count |  | Control total |  | Classification – Coloureds | Classification – Binaries | Classification – Multiples |  | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  | ***Performance Measurement Mechanism*** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Which of the following statements do you agree with?  Please tick one. |  |  |  |  |  |  |  | 10 |  |  |  |  |  |  |  |
| a | It is important to implement an IT balanced scorecard |  |  |  |  |  | 2 |  |  |  |  |  |  |  | IT performance management is important, regardless of whether a balanced scorecard is implemented or not. | 5, 9 |
| B | It is important to implement any performance management practice, whether in the form of a balanced scorecard or not |  |  |  |  |  | 8 |  |  |  |  | Accepted |  |  |  |  |
|  |  |  |  |  |  |  | ***490*** |  |  |  |  |  |  |  |  |  |

| | Critical | Very/Highly | Important/Valuable | Somewhat | None/Not at all | Count | Control total | Classification – Coloureds | Classification – Binaries | Classification – Multiples | Deduction | Cross-reference to Recommendations |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

| | Practice recommendations | Binary practice evaluations | Multiple practice evaluations |
|---|---|---|---|
| Accepted | 36 | 5 | 5 |
| Considered | 12 | | 2 |
| Not accepted | 1 | | 14 |
| Undecided | | 2 | |
| | **49** | **7** | **21** |