

https://dspace.org/

Realising Value with Information Technology Governance in the South African Public Sector

Williams, Zunaid

2011-06-24
http://hdl.handle.net/10539/10233

Downloaded from a DSpace repository. https://dspace.org/

Realising Value with Information Technology Governance in the South African Public Sector

Zunaid Williams

A research report submitted to the Faculty of Management, University of the Witwatersrand, Johannesburg, in partial fulfilment of the requirements for the Degree of Master of Business Administration.

Johannesburg, 2009

ABSTRACT

The role of Information Technology within organisations has changed materially over time. Information technology has become pervasive in almost all organisational processes and is the key component of most services that are provided by an organisation. The management and control of information technology has also had to adapt in order to ensure that Information Technology is able to continuously provide value to the organisation.

Within the public sector Information Technology has also evolved and is a key component of government planning and an operation as well as being a medium through which government is able to engage with the public. In order to ensure that the public sector is able to continuously generate value from Information Technology services and process, organisations will need to put in place an appropriate management and control system.

In order to gain an understanding of these methodologies semi-structured interviews were conducted with public sector representatives who elaborated on the specific structures, process and controls adopted by the organisations to ensure that Information Technology was able to deliver value.

The main finding of this research was that the most of the organisations had a general awareness of the impact of Information Technology on their operations, and had developed specific processes to ensure that there was alignment between the business and Information Technology plans. Furthermore the measurement and identification of the value generation capabilities of Information Technology were ascertained. The research also identified specific practices related to risk and performance management practices for Information Technology and there integration into the overall business frameworks.

Declaration

I declare that this research report is my own unaided work, except to the extent indicated in the acknowledgements, text and references. It is being submitted in partial fulfilment of the requirements for the degree of Master of Business Administration in the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in any other university.

_____

Zunaid Williams

Signed at _____ on this _____ day_____ 2009

Dedication

In memory of my Father Manuel Charles Williams (1951-2004) whose sacrifice and investment in my education will always be appreciated

Acknowledgements

I wish to express my sincere thanks to:

- Antony Soicher for his time guiding me through this process and always being accessible to advise me and allowing me to benefit from his experience
- All respondents who gave me their time to provide me with the information and knowledge at there disposal
- Graham Steenkamp for allowing me the time to complete this research
- My Wife, Shamima, for here support and sacrifices that she has made during this process
- My Sons, Aqeel and Yaqeen, who are the motivation for me continuing to improve myself

Table of Contents

ABSTRACT ii
Declaration iii
Dedication iv
Acknowledgements v
Table of Contents vi
List of Tables ix
Abbreviations x

Chapter 1 1

1. Introduction 1
1.1. Purpose of the study 3
1.2. Context of the study 5
1.3. Research Problem 6
1.4. Delimitation and limitations 6
1.5. Assumptions 7
1.6. Significance of the study 8

Chapter 2 9

2. Literature Review 9
2.1. IT Governance Overview 9
2.2. Need for IT Governance 11
2.3. The IT Governance Organisation 13
2.4. IT Business Alignment 18
2.5. Value Management 23
2.6. Risk Management 27
2.7. Legislation and Compliance 30
2.8. Literature Conclusion 37
2.9. Research Questions 39

Chapter 3 40

3. Research Methodology 40
3.1. Research design 42
3.2. Population and Sampling 43
3.3. Data Collection 44
3.4. Data analysis 45
3.5. Validity and reliability 46
3.5.1.Internal validity 46
3.5.2.Content Validity 46

3.5.3.External validity 47
3.5.4.Reliability 47

Chapter 4 48

4. Research results 48
4.1. Cognitive Maps 49
4.2. Research Finding 64
4.3. Organisational Findings and Process Maturity Evaluation 65

Chapter 5 98
5. Discussion of Findings 98
5.1. Review of research questions 99
5.2. Conclusion 116

Chapter 6 117

6. Conclusion 117
6.1. Introduction 117
6.2. Main Finding of the research 117
6.3. Recommendations for Management 120
6.4. Suggestion for further Research 121

Appendix A: Consistency Matrix 122

Appendix B: Interview List 123

Appendix C: Interview Questions 124

Appendix D: COBIT Maturity Matrix 125

Reference List 130

Table of Figures

Figure 1: Business Value Creation process 2

Figure 2: IT Governance Framework 3

Figure 3: IT Governance Positioning.....12

Figure 4: IT Governance Decision Areas 13

Figure 5: Cognitive Map for Interview 1.....49

Figure 6: Cognitive Map for Interview 2 50

Figure 7: Cognitive Map for Interview 3.....51

Figure 8: Cognitive Map for Interview 4.....52

Figure 9: Cognitive Map for Interview 5.....53

Figure 9: Cognitive Map for Interview 5.....53

Figure 10: Cognitive Map for Interview 6 54

Figure 10: Cognitive Map for Interview 6 54

Figure 11 : Cognitive Map for Interview 7 54

Figure 12: Cognitive Map for Interview 8.....55

Figure 13: Cognitive Map for Interview 9.....57

Figure 14: Cognitive Map for Interview 10 58

Figure1 5: Cognitive Map for Interview 11 59

Figure 16: Cognitive Map for Interview 12 60

Figure 17: Cognitive Map for Interview 13 61

Figure 18: Cognitive Map for Interview 14 62

Figure 19: Cognitive Map for Interview 15 63

List of Tables

Table 1: Organisation 1 Maturity Matrix 66

Table 2: Organisation 2 Maturity Matrix 68

Table 3: Organisation 3 Maturity Matrix 69

Table 4: Organisation 4 Maturity Matrix 71

Table 5: Organisation 5 Maturity Matrix 73

Table 6: Organisation 6 Maturity Matrix 76

Table 7: Organisation 7 Maturity Matrix 78

Table 8: Organisation 8 Maturity Matrix 80

Table 9: Organisation 9 Maturity Matrix 83

Table 10: Organisation 10 Maturity Matrix 85

Table 11: Organisation 11 Maturity Matrix 87

Table 12: Organisation 12 Maturity Matrix 89

Table 13: Organisation 13 Maturity Matrix 91

Table14: Organisation 14 Maturity Matrix 93

Table 15: Organisation 15 Maturity Matrix 96

Table 16: Domain Principles and Implementation Guidelines 112

Abbreviations

AIA	- Access to Information Act 2000
BSC	- Balanced Scorecard
CEO	- Chief Executive Officer
CIO	- Chief Information Officer
COO	- Chief Operating Officer
COBIT	- Control Objective for Information and Related technology
ECT	- Electronic Communications and Transactions Act 2002
EDI	- Electronic Data Interchange
ISACA	-Information Systems Audit and Control Association
IT	- Information Technology
ITG	- Information technology governance
ITGI	- Information Technology governance Institute
MIOS	- Minimum Interoperability Standards
NIST	-National Institute of Standards and Technology PFMA
PFMA	- Public Finance Management Act 1999
MFMA	- Municipal Finance Management Act 2003
SA	- South Africa
SLA	- Service Level Agreement
SITA	- State Information Technology Agency
SOX	-Sarbanes-Oxley Act

Chapter 1

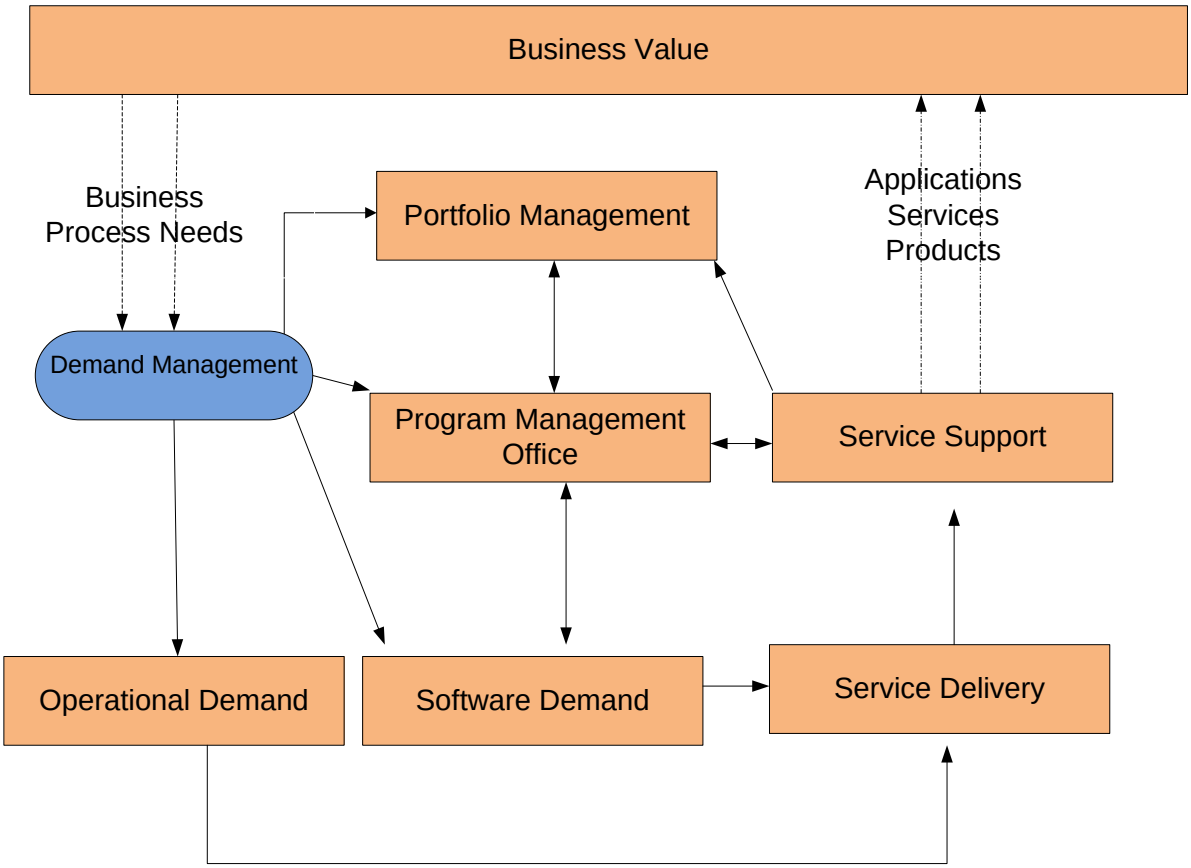
1. Introduction

Information Technology (IT) has become integrated into the overall functions and processes of organisations, this has resulted in a more strategic role for information management and control in organisations. Many organisations are changing their operational processes using IT services to achieve productivity and operational efficiencies (Davies, 2004). Therefore the selection of the appropriate management methodology is critical for improving organisational effectiveness (Davies, 2004). According to Porter (1985) IT was seen as supporting the business processes that made up the company value chain. However today IT no longer provides a supporting role but is viewed as a vital enabler for generating value as it pervades all aspects of the organisation (Sharif, 2006).

Research conducted by Gantin (2006) argues that in order for the organisation to derive value from IT operations, it is imperative that an appropriate IT structure be adopted in order to oversee the management and control. This structure Gantin (2006) contends will ensure that IT delivers value to the organisation by ensuring, Business-IT alignment, executive sponsorship for IT, effective risk management and a framework to manage IT investments.

According to Mercury (2006b) value is generated through the utilisation of IT services as indicated in figure 1 below. However in order for value to be realised, Mercury (2006b) argues that an IT governance framework has to be adopted by the organisation to ensure that the initial organisational requirements are effectively managed throughout the process to deliver the expected value.

Figure 1: Business Value Creation process



Source: Optimize IT Governance: Optimize the business outcome of IT, www.mercury.com, 2006

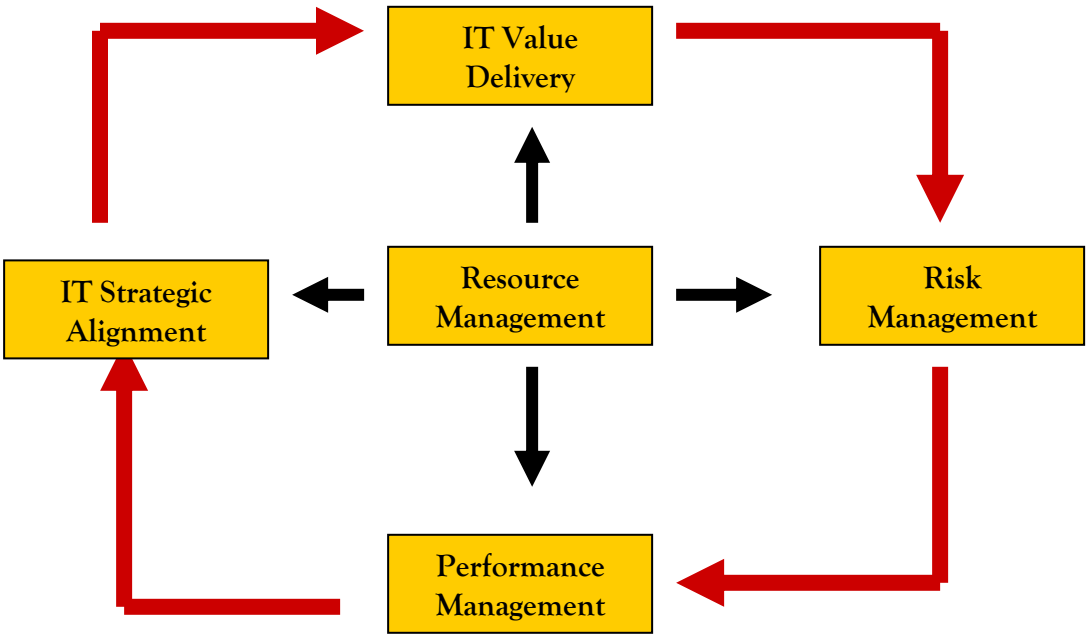
In addition to ensuring that there is an alignment between the organisation's needs and the execution and delivery of IT services to the organisation, the Information Technology Governance Institute (ITGI) argues that value is derived from IT in organisations that are able to adapt to the regulatory environment in which they operate (ITGI, 2005a). According to the ITGI (2005a) organisations have to understand and ensure compliance with operational standards as well as with legislation governing the management of information in the operational territory.

1.1. Purpose of the study

According to the Information ITGI (2005a) IT Governance is focussed on five domains. These domains as depicted in figure 2 include:

- IT Strategic Alignment
- IT Value Delivery
- IT Resource Management
- IT Risk Management
- IT Performance Management

Figure 2: IT Governance Framework



Source: Van Grembergen, W. (2004): Strategies for Information Technology Governance, Ideas Group, London

The ITGI (2005a) believes that through IT Governance the ability of IT to deliver value to the business can be enhanced. The ITGI (2005a) believes that governance is driven by the strategic alignment of IT with business as well as the management of risk and technology investment planning.

The purpose of this research is to understand the role that IT Governance practices plays in ensuring that information systems deliver value to organisations. In order to achieve this outcome a review of the current literature will be conducted to determine best practices in IT Governance. The research phase will focus on the current IT Governance practices within public sector organisations. Our recommendations and conclusion will focus on what is the most popular format for these domains. The researcher's aim in this study is identify the key practices related to IT Governance which will enable organisations to better understand what is required in terms of IT Governance in order to generate value.

1.2. Context of the study

Dahlberg and Kivijarvi (2006) argue that more emphasis has been placed on IT Governance in recent years with researchers and practitioners focusing on the need to ensure that more accountability and responsibility is taken for the control and operation of information systems in the organisation This Dahlberg and Kivijarvi (2006) contend is due to the fact that IT has become an integral component in an organisation's ability to achieve its goals and it is therefore imperative that the performance of IT be managed and controlled.

Globally organisations have been compelled to review their attitude toward IT management due to the introduction of legislation that has required them to ensure that their systems are able to provide the business with the relevant information that will allow managers to make decisions with the most recent and pertinent information (Damianides, 2005). In the United States the introduction of Sarbanes-Oxley (SOX) as part of the review on disclosure practices for public entities has firmly put the responsibility of information systems control in the hands senior managers (Damianides, 2005). Multinational financial services organisations have seen the introduction of Basle II which similarly required more attention to be paid to the management and control of information systems in order to produce a true reflection of the financial performance and operations of institutions. (Damianides, 2005)

There has also been a drive globally to implement best practice methodologies in the area of IT Governance (ITGI, 2005a). The Information Systems Audit and Control Association (ISACA) has developed The Control Objectives for IT (COBIT), a control framework that allows organisations to implement a system where domains of authority and processes have been defined. This framework also allows organisations to measure and evaluate the progress that they are making in implementing an effective governance system (ITGI, 2005a).

In South Africa 90% of respondents to a recent survey conducted, perceived IT to be critical to achieving their organisations` objectives, of this group, 55% were involved in IT governance initiatives such as risk management, information security, IT resource budgets, IT service management strategies as well as establishing standards and frameworks (Senne, 2006)

1.3. Research Problem

According to the ITGI (2003) organisations are able to achieve value from IT initiatives through the alignment of organisational strategy, the management of risk and the management of IT investments. The purpose of this research is to investigate the IT Governance methodologies adopted by South African public sector organisation in order to deliver value.

1.4. Delimitation and limitations

Due to the number of respondents that were approached for this study the statistical validity of the research may be limited. Currently this study only wishes to identify those issues that are appropriate in ensuring that IT Governance provides value.

This study was limited to organisations that the researcher was aware of that currently have formal IT management structures and processes in place. The researcher endeavoured to contact knowledgeable individuals in the target organisations involved in IT Governance but limited the scope of the study to the areas of IT value, control, performance and risk.

1.5. Assumptions

The following assumption were used while doing this research

a) All participants involved in this study are aware of or have been exposed to IT Governance practices formally or informally

b) The processes that are used in the development of the IT Governance framework can be generalised across the various industries in South Africa and the terminology will be understood by respondents in the public sector.

c) Organisations are aware of the regulations which relate to the management of information in South Africa

d) The respondents to the survey were all involved in the overall management and control of IT within there environments

e) The respondents to this survey were all in a leadership position within the organisation and were therefore aware of the importance and role of IT to their organisations.

1.6. Significance of the study

According to van Grembergen (2004) organisations implement IT Governance in order to ensure that they are able to achieve value from IT initiatives. Furthermore, van Grembergen (2004) argues that the realisation of value from IT is accomplished through the development of strategic flexibility allowing organisations to adapt to the complex environment in which they operate.

This study will assist public organisations to gain a better understanding of the practices that are essential for ensuring that IT initiatives add value to the business, and control the risks that may arise from technology investments.

The role of factors that are unique to the South African environment will also be investigated. Legislation and industry standards which are requirements for information management in South Africa will be reviewed. In addition how organisations are able to ensure that these factors are integrated into control and management initiatives will be assessed.

Finally the identification of the key processes and principles that create value will be assessed which will allow management to develop a blueprint which can be used to ensure that IT is managed effectively in the organisation.

Chapter 2

2. Literature Review

In order to gain an understanding of what IT Governance actually entails it is important to gather information from previous work on the subject. The areas of focus that were covered in this review include:

- The structure of IT Governance in organisations
- Best practices and processes being used in IT Governance
- The role of relationships and communications between Business and IT
- The process of aligning business and IT
- IT Value Management and;
- IT Risk Management

2.1. IT Governance Overview

According to King (2006), governance, is the principle of running a business ethically and responsibly. The aim is to lower the risks for investors and increase profitability in a way that shows respect for the environment and the people of the regions in which it operates, this same approach needs to be adopted in the control of IT. King (2006) believes that the main purpose of the organisation's senior management is to manage risk and to provide investors with a return. Similarly in IT Governance the relevant managers need to ensure that the systems that the company depends on in order to be productive do not place the organisation at a disadvantage and that any investment that is made in IT will be of value to the organisation objectives (King, 2006).

Selig (2006) contends that the extent of IT Governance in an organisation is depended on a number of factors. These include the budget available for IT investments, the dependence of the organisation on IT for their business processes, the organisation's appetite for risk and innovation and the organisation's framework in addressing issues of regulation and compliance.

According to Selig (2006) Effective IT Governance is critical for business success and is beneficial in formalising the oversight and accountability of organisational management. In addition the formal processes and structures that are derived from the development of an IT framework will improve the planning and communication processes and allows IT to collaborate more effectively with the business (Selig, 2006).

2.2. Need for IT Governance

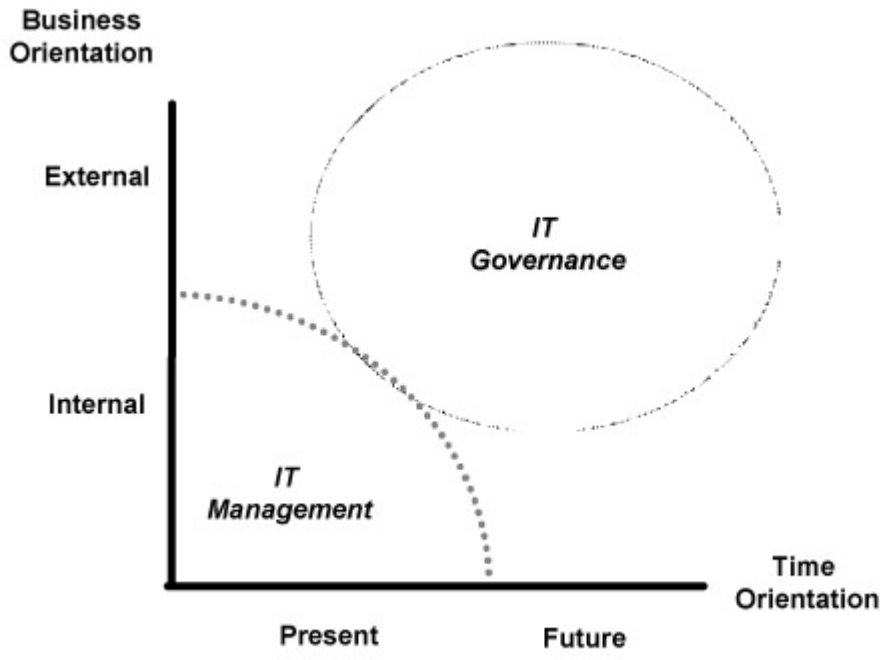
Pultorak (2005) argues that IT Governance is required to address three critical areas; these are conformance, performance and responsibility. Conformance addresses the action required to adhere to the relevant regulatory requirements. The main aim of conformance is to minimise risk to the organisation. Governance boards need to ensure that the organisation meets their legal, contractual and regulatory obligations (Pultorak, 2005). Performance is related to the efficiency and effectiveness of the IT process in order to ensure that the business meets its business objectives and to ensure the long term viability of the business. Relating responsibly addressed the question of assigning actions to the appropriate stakeholders and providing them with feedback. Pultorak (2005) maintains that to ensure consistency in the execution, monitoring processes need to be instituted to continually measure performance through a management system and periodically through auditing the processes.

Due to the importance of IT Dahlberg and Kivijarvi (2006) believe that managers should provide the necessary leadership, organisational structures and processes for IT Governance in the organisation. Mercury (2006c) is also of the view that a strong leadership is essential to a successful governance implementation. If the business leadership's attitude to governance is not positive, this mind-set will pervade throughout the organisation.

King (2006) argues that the need for the executive to become more involved in the technology strategy of the company has taken on more significance as a result of the information age, where company assets such as intellectual property has become just as valuable as the tangible assets that are declared on the company balance sheet. King (2006) also believes that IT provides the transparency that organisations require in the disclosure of information to all relevant public and private stakeholders. For this reason King (2006) believes that it is the responsibility of the senior managers to take control of the technology strategy of the organisation. The protection of information assets is vital in this era in order to ensure that only authorised and trusted individuals have access to information that could place the company at a serious disadvantage if the competition or public became aware of it. In order to do this IT managers need to be elevated to senior management status so that there is a direct line of reporting to the Chief Executive Officer (CEO) who can then take ownership of the technology strategy of the organisation (Feeney, Edwards, Simpson, 1992).

Peterson (2004) argues that IT Governance is not just a new form of IT management. Peterson (2004) whose view of IT Governance is depicted in figure 3 argues that, Governance has the dual responsibility of positioning IT to meet future objectives by understanding how IT needs to transform itself to adapt to the changing environment in which business operates and also incorporating IT management which is focussed on the efficient and effective supply of IT services to the business.

Figure 3: IT Governance Positioning



Source: Van Grembergen, W. (2004): Strategies for Information Technology governance, Ideas Group, London

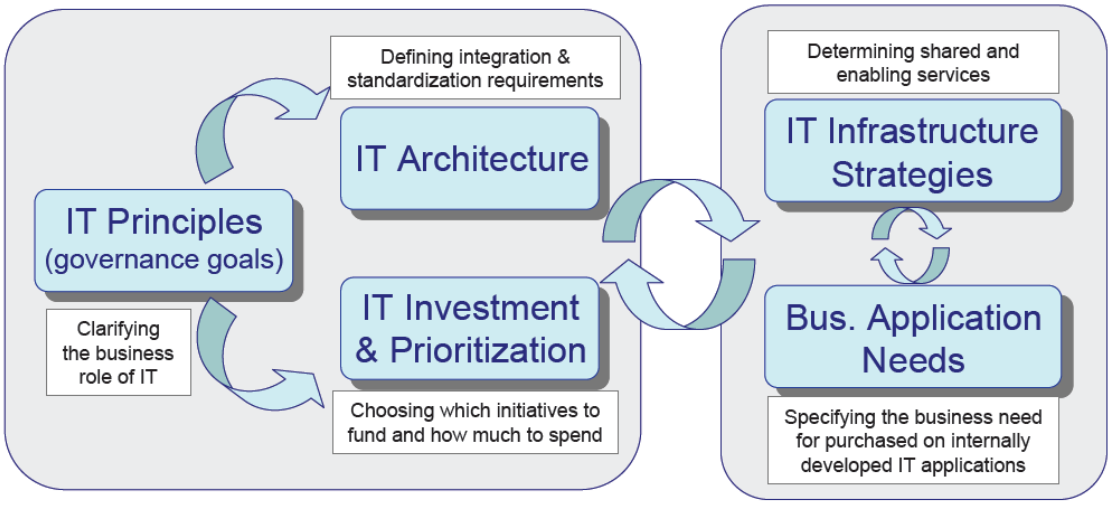
Oettinger and LeGates (2000) argue that IT Governance committees need to set the vision of IT within the organisation. These committees need ensure that IT delivers high quality, highly efficient and predictable levels of service that needs to be managed in business terms. If the governance committees are able to achieve this then they will ensure that the organisation reaches a level of operational excellence.

2.3. The IT Governance Organisation

In order to understand IT Governance operations we need to review the various models, which influence governance initiatives. According to Dahlberg and Kivijarvi (2006) studies conducted by Brown and Magill (1994) and Sambamurthy and Zmud (1999) determined that IT Governance structures were contingent on the Corporate Governance structure, economics of scope and the business' IT capabilities.

Weill and Ross (2005) argue that an organisation needs to implement a structure of governance that will cover any of the five areas of decision making. Weill and Ross (2005) propose that decision making activities of the governance board as depicted in figure 4 below, cover IT principles, IT architecture, IT Infrastructure Strategies, Business Application Needs and IT Investment and Prioritisation.

Figure 4: IT Governance Decision Areas



Source: Weill, P. and Ross, J. (2005): A Matrixed Approach to designing IT Governance, MIT Sloan Management Review

Weill and Ross (2005) contend that it is the duty of the governance board to define the role of IT in the business. The board would therefore need to understand the core business processes of the organisation and analyse the information needs that drive these processes as well as review what IT services are the most critical for the organisation to achieve its objective (Weill and Ross, 2005). The board would also need to determine the technical capabilities and platforms needed by the business and ensure that an appropriate service level agreement is drawn up. Furthermore the board has the

responsibility of determining what the most critical projects are that will support the organisations drive to achieve its objectives (Weill and Ross, 2005).

Dahlberg and Kivijarvi (2006) argue that IT Governance decision making is best approached through a systematic process. The emphasis in their approach is on the structures and processes that are utilised to control the IT related operations and projects in the organisation. Through the adoption of this framework Dahlberg and Kivijarvi (2006) believe that organisations will be able to implement adequate budgetary control over IT, improve the utilisation of IT related assets and resources and improve the ROI of IT related projects.

Systematic approaches to IT Governance structures are mainly defined as centralised, decentralised or a hybrid (federal) systems (Peterson, O'Callaghan and Ribbers, 2000). Depending on the configuration of the governance framework, Peterson (2000) contends that the role players take on different functions in the governance organisation. In the centralised approach, all decision making authority is vested in the hands of the corporate managers while business units will have control over applications, services and resources in a decentralised structure (Peterson, 2004). The benefit of the centralised approach according to Peterson (2004) is that organisations achieve greater consistency and standardisation which leads to improved economies of scale. Whereas in a decentralised model, lines of business are more flexible and are able to adapt to changes a lot easier.

In the federal system the underlying infrastructure is under the control of the executive team while the business unit has complete control over the applications which they wish to utilise with the proviso that it is compatible with the underlying infrastructure (Peterson, 2004). The federal system is further delineated into IT centric and business centric approaches depending on which manager's view of the business is more relevant. In an IT centric environment the IT management are responsible for the control of business applications whereas in the business centric model business units are involved in the development and structure of the IT applications (Peterson, 2004).

According to Peterson (2001) the adoption of an IT portfolio management system enables the organisation to implement an effective governance structure, in this way the organisation can handle all there strategic planning issues as the portfolio ensures a clear differentiation of responsibilities and lines of control. The development of the IT Portfolio within an organisation according to Peterson (2001) indicates that there is an institutionalisation and formalisation of the IT Governance processes within the organisation.

This formalisation ensures that IT decision making mechanisms will now adopt the rules and procedures of the organisation (Van Grembergen, 2004) in this manner the guidelines that have been driven from corporate governance are adopted by IT Governance. A further characteristic of formalisation according to Peterson (2001) is the development of structures and processes that provide managers with a channel in which to communicate and share information, therefore all stakeholders will understand what they are personally accountable for. This delineation of control ensures that IT decision making is made according to business rules and they provide a roadmap for the achievement of business objectives

Peterson (2004) believes that the character of the IT Governance structure in the organisation is the product of how controls are applied to the IT portfolio in terms of IT Investments, IT Applications, IT Services and IT Resources. The main objective of a portfolio management approach is to strategically and tactically deliver value, through the optimisation of enterprise investments, and lay the groundwork for a technologically sophisticated business strategy.
According to Gerrard (2006b) governance can be delineated between demand and supply governance. Demand governance is all those processes that are focused on strategy and planning whereas supply governance is focused on IT operations.

The primary responsibility of demand governance is related to how business focuses on defining the goals of the IT organisation. IT demand governance is also concerned with the style and structure of governance in the organisation as it pertains to decision rights. Gerrard (2006b) sees IT demand governance as focused on the business investment decisions and strategic planning functions that are related to the IT organisation of the business. These investment and planning decisions that are made by

the various stakeholders in the IT Governance environment need to take into cognisance the style and culture of the organisation in order to ensure the alignment of business and IT.

Gerrard (2006b) argues that IT demand governance needs to be cognisant of the culture and aligned with the overall decision making perspective in the organisation. The ability of the organisation to leverages its IT potential combined with the style and competitive posture of management, Gerrard (2006b) believes will greatly affects the role of IT and the organisation's willingness to invest in a governance framework. Research conducted by Mercury (2006a) supports Gerrard's (2006b) view, as they assert that governance can only succeed in the company if the managers are able to understand and manage the culture of the organisation. In order to implement a governance framework managers and practitioners need to be mindful of how thing are actually done in the organisation. The style of governance in the organisation has to relate to the way in which business units in the organisation relate to each other.

IT demand governance is also concerned with the deployment and management of scarce resources in the organisation (Gerrard, 2006b). This is a key area of concern for IT managers who need to manage a scarce pool of resources while prioritising those projects that will add the most value to the business. It is therefore essential that these IT managers understand the strategic direction of the company when planning IT projects and reviewing funding mechanisms.

IT supply governance is more concerned about the execution of responsibilities within the various technology domains that the organisation is depended on. Gerrard (2006b) sees IT supply governance falling into the four specific areas of planning, implementation, management and monitoring. Prior to planning however, the IT supply governance mechanisms of the company needs to develop policies that will govern IT in the various technology areas. The policy planning initiative needs to take into consideration the views of the various stakeholder groups and develop policies that are based on excepted frameworks such as COBIT (Gerrard, 2006a). Once these policies have been adopted the IT supply organisation would need to define operational procedures and codes of conduct for the various IT domains. These codes and procedures are usually articulated through service level agreements or performance management systems (Gerrard, 2006a). Scheduled review and assessment periods need to be defined by IT supply governance in order to ensure that the processes are being adhered to and the IT Governance plan is on track.

During the implementation of IT Governance initiatives organisations should always ensure that they are able to implement policies that are in sync with the organisations culture and style (Calder and Watkins, 2005). This is necessary as Calder and Watkin (2005) believes that this will ensure acceptance in the organisation and limit the resistance to it. The policies and processes will also need to be well understood by the organisation so that they can be reviewed for their effectiveness in the organisation.

2.4. IT-Business Alignment

Tavakolian (1999) conducted a survey into evaluating the link between IT structure and organisational competitive strategy. The results of this study found that there was a close alignment between IT structure and business strategies and therefore strategy was an important determinant in IT control structures. This study indicated that IT structure and the type of control structure were strongly related to the organisations competitive strategy. According to Tavakolian (1999) different IT structures seem to fit different competitive strategies. In current practice this was also depended on the level of risk an organisation was willing to take in its strategy. Tavakolian (1989) found that users in conservative organisations had less responsibility for their IT activities than the users in aggressive organisations. The conclusion that can be drawn from this study is that depending on the risk profile of the company a centralised governance model will be adopted by conservative companies while aggressive companies will allow business units more autonomy and are more characteristic of a decentralised or federal approach.

Gerrard (2005) argues that in order to be effective IT needs to understand the expectation of each line of business in the organisation. According to Gerrard (2006a) the role of IT in the organisation is defined by two dimensions. Firstly it needs to look at the strategic competitive positioning of the business in terms of the organisations risk profile. On the other continuum is the view from business about the role that IT needs to play in the organisation. On the one end business sees IT playing a strategic and transformational role where IT enables the business processes, while others view IT as only tactical and provides utility services to support the business operations.

The strategic alignment model proposed by van Grembergen (2004) defines IT strategy as a product of internal control and external positioning. According to van Grembergen (2004) successful IT and business alignment is achieved when the organisation has a good understanding of how the IT systems have to be configured and managed within the organisation in order to take advantage of the organisation's competitive position in the external IT marketplace. Albrecht and Pirani (2004) argue that through governance the organisation is able to remove the silo syndrome of operations in the organisation and reinforces the need to communicate to achieve business objectives.

When the business and IT are in alignment and are effectively collaborating, the business is able to achieve a degree of innovation that provides them with a competitive advantage in the marketplace (van Grembergen, 2004). This innovation is achieved when the IT organisation is able to leverage both the service delivery and solution integration capabilities to deliver operational excellence (van Grembergen, 2004). However according to van Grembergen (2004) this can only be achieved if the key stakeholders involved in IT Governance are able to understand what the critical business value drivers are, and how IT can act as a catalyst to increase the potential of these drivers.

According to Luftman and Brier (1999) the alignment of IT and business are contingent on enabling and inhibiting factors. If the enabling factors are more evident in the organisation there is a better chance for IT and business to be aligned. The enabling factors for business IT alignment include manager support for IT, IT's involvement in business planning and the prioritisation of IT projects based on IT understanding the business issues. Inhibiting factors that could prevent business IT alignment includes IT failure to meet commitments and a lack of understanding of business issues by IT. Luftman and Brier (1999) argue that alignment of business and IT has specific components in the business strategy and operational domains.

In term of the business, scope alignment occurs when IT is able to allow the business to be meeting the need of their clients. Rahman and Purushottam (2004) support this view as they see alignment occurring where IT does not constrain the business operation but rather support the business so that it can operate and grow according to its own strategy and plans.

In the implementation of an IT Governance system Dahlberg and Kivijarvi (2006) propose that the first step in accomplishing alignment, is to ensure that there is coordination between the objectives of the business with the systems and projects that the IT organisation is developing. This coordination is achieved through agreeing with IT on the goals and targets that the IT organisation has to achieve in order to support the business. It is also critical at this stage to define the activities, and the required resources needed for IT to assist the business strategy. A comprehensive risk assessment for IT is also needed during this initial stage so that managers can understand the threats that IT may face in achieving their objectives (Dahlberg and Kivijarvi, 2006).

According to Brown and Magill as cited in Dahlberg and Kivijarvi (2006) the alignment of business and IT is accomplished through the interaction between business and the IT organisation in discussing IT investments. According to this study the knowledge and experience that each person is able to provide in the IT planning process will ensure that the IT infrastructure is able to support the operations of the organisation.

Broadbent and Weill (1999) contend that the alignment between business and IT is achieved by having consistent practices in four areas. The areas are firm wide strategy formation processes, technology strategy, organisational structures and capabilities, and Information systems responsibilities and policies (Broadbent and Weill, 1999). Broadbent and Weill (1999) also argue that IT and business alignment is possible if certain practices are implemented in the organisation. These practices included processes that identified implementation responsibilities as they related to the strategy formation process. A strong communications process also needs to be implemented so that firm wide strategies are communicated at all levels and also reviewing management practices so that it could take advantage of technology enhancements.

In order to achieve alignment Weill, Subramani and Broadbent (2002) argue organisations need to be strategically agile in IT decision making. Organisations that can determine the type of agility it will need

for specific business initiatives are more likely to make sensible infrastructure investments. These investments ensure that IT infrastructure is integrated across business units allowing the organisation to take advantage of shared IT capabilities creating a platform for all business processes. These capabilities comprise both technology and human factors.

Oettinger and LeGates (2000) believe that for governance to be effective in an organisation, alignment between business and IT needs to be established at different levels in the organisation. The objective Oettinger and Legates (2000) contends is that senior management are satisfied that all business units are talking to IT as the strategy evolves so that the infrastructure can adapt to the changing environment. In order to successfully implement a governance structure in the organisation Oettinger and LeGates (2000) assert that behavioural and procedural aspects need to be addressed. This aspect involves having the ability to manage projects and developing new practices for reporting. For Oettinger and LeGates (2000) these steps need to be done gradually so that people can familiarise themselves with the new formats. Oettinger and LeGates (2000) also believe that the automation of business processes will aid the successful implementation of governance. This is essential so that skilled resources can spend more time on analysis and decision making activities.

According to Coupe (2006) a critical element of business–IT alignment is the selection of standards by the organisation. The type of standards that are selected by the organisation will have an impact on the operating models that are to be deployed by the organisation. According to Coupe (2006) the selection of these standards are driven by business users who are more concerned with functionality rather than whether it complies with specific protocols. The role of standards in the organisation also needs to incorporate an oversight function that ensures that the company does not forget their fiduciary, legal or quality responsibilities in the selection of the service.

Simonsson (2006) endorses the view of Weill (2004) who asserts that the role of IT Governance is to provide strategic decision making as it relates to IT Governance. Simonsson (2006) believe that IT Governance decision making should revolve around the four dimensions. In terms of goals the governance board would need to look at issues such as setting the IT direction for the organisation and aligning this with policies that will ensure that resources are fully aware of their deliverables. Process decisions for Simonsson (2006) are related to defined work standards and action plans that need to be implemented. While people decisions are concerned about identifying the relevant skills and ensuring

that training and skills transfer programs are in place (Simonsson, 2006). Finally technology decisions are concerned with the types of systems that need to be deployed and the configuration of these systems (Simonsson, 2006). For Simonsson (2006) all decisions taken with regard to IT need to be investigated, discussed and transformed into deliverables for the relevant stakeholders.

2.5. Value Management

According to (Tallon, Kraemer and Gurbaxani ,1999) the value creation process of IT in the business can be viewed from an economic perspective as well as from an operational perspective. In economic terms the value derived from IT is measured in most cases in terms of the single dependent variable of productivity. The productivity gains that are achieved through the implementation of IT systems, Tallon, Kraemer and Gurbaxani (1999) argue is usually justified with traditional financial modelling and business justification tools such as; cost-benefit analysis, Return on investment, Return on assets and Net present value.

Tallon, Kraemer and Gurbaxani (1999) argue that the reason why organisations are focused on measuring the economic value of IT is due to the objectivity which it provides. The problem with economic measures of IT value though is that they do not take into consideration the intangible benefits that can be derived from IT systems such as improved product and service quality (Tallon, Kraemer and Gurbaxani, 1999).

From an organisational perspective, Tallon, Kraemer and Gurbaxani (1999) have identified the operational effectiveness that can be derived from systems as key to IT value creation. According to Tallon, Kraemer and Gurbaxani (1999) organisational measures of IT value are seen in terms of new product developments, product quality, service quality and customer satisfaction.

The ITGI has developed the VAL-IT framework in order to support COBIT, in order to drive the value of IT from a business and financial perspective. This framework identifies three key management practices as critical for IT to deliver value to the business. These three practices are value governance, portfolio management and investment management. This model emphasises the need for governance processes to cover business alignment in terms of cost and benefits, financial and non-financial as well as risk since they play a key role in all investment analysis practices

According to the ITGI (2006) IT investments are no longer about just implementing IT solutions, and more about implementing solutions that transform the nature of the organization. ITGI (2006) believe

that IT enabled business investments can bring huge rewards if the appropriate governance structures and management processes are put in place.

The value framework proposed by the ITGI (2006) is based on seven underlying principles. According to these principles, IT investments should be based on a portfolio management framework and will include the full scope of activities that are required to achieve business value. Furthermore the principle of total cost of ownership is espoused as IT-enabled investments need to be managed through their full economic life cycle.

In terms of value delivery practices, the VAL-IT framework proposes that organisations take into account the nature of the project and adopt the appropriate mechanism for evaluating its benefit to the organisation. These practices would also need to ensure that the critical components of all projects are identified up front and that all problems or changes to projects will be addressed immediately if they endanger the benefits to the organisation. It is also critical that in order to deliver value to the organisation IT engages with all stakeholders and assign appropriate accountability for the delivery of capabilities and the realisation of business benefits. The final principle of the framework suggests that in order to ensure IT value, processes are continually monitored, evaluated and improved.

Through the implementation of value management the ITGI (2006) contends that organisations will be able to measure and monitor their return on investment for IT-enabled solutions. Through the use of value governance the ITGI (2006) believes that organisations will be able to optimise their investments in IT. The main focus of value governance is to provide a strategic direction for the technology investments of the organisation and also to define the investment portfolio characteristics.

The goal of portfolio management according to the ITGI (2006) “is to ensure that an organisation’s overall portfolio of IT-enabled investments is aligned with and contributing optimal value to the organisation’s strategic objectives” (p14). According to the ITGI (2006) this is achieved by establishing and managing resource profiles, ensuring the investment thresholds are defined, evaluating and prioritising IT projects and ensuring that an adequate reporting structure is in place.

The projects that are selected as part of the organisation's portfolio, needs to be actively managed throughout their full economic life cycle in order to ensure that the value of these projects are optimised (ITGI, 2007). In order to ensure the success of these projects part of the portfolio management process includes ensuring that the right resources are allocated to the projects, problems are identified early and corrective action is implemented (ITGI, 2007).

The purpose of investment management as part of the value management framework is to ensure that the IT-enabled investment programmes of the business are able to deliver optimal value at an affordable cost with a known and acceptable level of risk (ITGI, 2007). In order to ensure that the process is completed successfully it is essential that people working on the project identify the business requirements of the organisation and develop a clear understanding of the business needs (ITGI, 2007). Once the requirements are clearly understood it may be necessary to develop a business case for the project where the details of the risks, costs and benefits are documented. It may also be an advantage for the business to asses the alternative options that the business has when they are looking at a particular project (ITGI, 2007). It is also critical that clear accountability and ownership is delegated to all stakeholders who will participate in the IT- enabled projects (ITGI, 2007).

Di Maio (2003a) argues that beyond the measures identified above, within the public sector the value that is derived from IT should also be considered in terms of its political impact and service provisioning to the constituents. According to Di Maio (2003a), the concept of public value needs to support the role that government plays within the society at large.

According to Di Maio (2003a) government takes on different roles in their interaction with citizens. In the first instance government is the primary representative of the citizen and needs to be available to respond to the needs of the constituents. Government also needs to provide protection to their citizens both from a security and economic point of view and needs to ensure that the information that supports this role instils confidence in the public. Finally government's role in providing service and infrastructure to the public needs to be supported by information that improved planning (Di Maio 2003a)

Di Maio (2003b) has also identified standards through which IT Value can be assessed based on there service to the constituents. In terms of strategic alignment, IT should enhance links with the public and establish new channels through which government can interact with the public (Di Maio, 2003b). From a process impact perspective, IT should ensure that existing data can be used on multiple platforms to support delivery, this should therefore have a direct payback by ensuring fewer complaints (Di Maio, 2003b). The architecture principles adopted by government should also allow IT to link with external parties to improve their own services (Di Maio, 2003b).

Di Maio (2003b) identified similar standards in terms of political return that can be attributed to IT. From a strategic alignment perspective, IT should support the organisation's ability to adapt to a changing regulatory environment thereby ensuring that operational processes are able to adapt as well (Di Maio, 2003b). IT should also have a direct payback in terms of improving the organisations corporate image and ensuring that objectives can be met by implementing automated process to improve services (Di Maio, 2003b).

2.6. Risk Management

The National Institute of Standards and Technology (NIST) define IT risk as an adverse event that has the potential to be detrimental to the operations of the business (2005). According to van Grembergen (2004) a critical component of the management and control function within IT is the implementation of a comprehensive risk framework. The ITGI (2007) believes that assessing and managing the risks within the IT environment is essential for satisfying the business requirement of understanding the potential impact of a threat within the IT environment to the business' processes, goals and objectives. The ITGI (2007) assert that the potential impact on the goals of the organisation which is the result of an unplanned event has to be identified, analysed and assessed.

According to Gerber and von Solms (2005) successful IT risk management is based on examining the threats to the IT environment's information, systems and processes. Through this process the organisation would need to ensure that they are able to identify high priority risks as they relate to critical business processes, and adopt an intervention strategy that is acceptable to the business (Gerber and von Solms, 2005)

Bandyopadhyay, Mykytyn and Mykytyn (1999) developed a comprehensive IT risk framework in which they had identified threat to the organisation as being both internal and external and were also classified as technological, human, natural or environmental. According to the work done by Bandyopadhyay et al (1999) risks also needs to be classified at the application, business unit and organisational level as each level has a different impact on the overall functioning of the business, and would therefore have a different degree of acceptability and priority in the business and as such the investment in managing these risks would vary.

According to Rassmussen (2006) the management of risk within the IT environment needs to be transformed from tactical where only information security and compliance are focussed on and needs to be integrated into the overall risk management process of the business. Organisations that adopt this approach also achieve better alignment between the objective of the organisation and IT, and IT and business are able to both understand the challenges that they are faced with (Rassmussen, 2006).

The NIST (2005) also identified various role players in the organisation who they believed should all be involved in the IT risk management process. According to the responsibilities matrix identified by the NIST (2005), the senior management in the organisation should ultimately be responsible for the risk in the IT environment and should ensure that the required resources are available to ensure that the organisation develops the capabilities to resolve any threats (NIST, 2005). Senior management are also responsible for ensuring that policies are developed that will protect the organisations assets (ITGI, 2007).

In terms of the role that IT play in the risk management process, the NIST framework (2005), indicated that it was the duty of the Senior IT office to ensure that the appropriate planning and budgeting be done to implement risk plans. Senior management are also responsible for ensuring that policies are implemented to protect the IT environment (ITGI, 2007). The personnel within the department are then responsible for ensuring the appropriate controls are implemented to ensure the integrity, confidentiality and availability of organisational information (NIST, 2005).

In developing an IT Risk strategy, organisations also need to ensure that the system that is adopted needs to be aware of risks over the entire life of the IT entity (Olzak, 2008). According to Olzak (2008) risks need to be identified early in the life of the system or process and need to classified as either project or operational risks. The adoption of this approach ensures that the long term cost associated with implementing the appropriate intervention will be reduced (Olzak, 2008).

Bandyopadhyay (1999) as well as the NIST (2005) has recommended that a systematic approach be adopted to the management of risks within the IT environment. According to Bandyopadhyay (1999) the management of risks within the IT environment should follow a sequential process that encompasses risk identification, risk analysis, risk mitigation and risk monitoring.

During the risk identification phase, organisations need to ensure that they are able to identify all possible eventualities that could possibly endanger the operation of an IT service (Bandyopadhyay, 1999). These threats should not only be considered in terms of deliberate action that could be taken against the organisation, scenarios that take into account the inadvertent actions that may result in the loss or damage of organisational information assets should also be considered (Bandyopadhyay, 1999).

Once the risk have been identified the organisation as a whole needs to consider the impact of the threat on the organisation's operations (Bandyopadhyay, 1999). According to the NIST (2005) the process involves assessing the potential risk as well as determining the probability that this may occur. The output of this process should ensure that the organisation has identified appropriate controls for reducing or eliminating the risk.

During the risk mitigation phase, organisations need to consider fully the various counter measures that they have at their disposal to address a risk (Bandyopadhyay, 1999). The process involves considering both the cost of the related countermeasure and determining whether the investment is reasonable considering that the event may occur if no investment were made (Bandyopadhyay, 1999). The final phase of the approach involves monitoring the risks as well as the process. (Bandyopadhyay, 1999). The monitoring process allows the organisation not only to adapt there processes in order to incorporate new risks but also to reduce cost in areas where risks no longer pose the potential threat they once did.

2.7. Legislation and Compliance

The main mechanism that is used by organisations to deliver on their mandate to implement an effective governance framework is the COBIT model which was developed and maintained by ISACA (Salle 2004). The COBIT framework was developed in 1998 and has successfully been able to break down the management and control of IT infrastructure into four operational domains with thirty-four different processes (Salle 2004). This framework has been generally accepted as a best practice model for the implementation of IT Governance (Bakker, 2006).

The four domains that are covered by this framework are.

- Planning
- Acquisition
- Implementation
- Monitoring and Control

Through the use of the COBIT framework, organisations are able to implement an IT Governance framework which covers the fiduciary, security and quality requirements that are necessary for most large organisations (Salle, 2004). According to van Grembergen (2004) these requirements are achieved due to COBIT's focus on key competencies.

The COBIT framework assesses the IT functions effectiveness in delivering information to the business that is pertinent and relevant to the related business process. The accuracy, usability and timeliness of the information are also critical (ITGI, 2007). Furthermore the efficiency of the IT processes and the ability to utilise the organisational resources optimally and leveraging each asset's key strength in order to deliver the right information to the organisation are also seen as critical (ITGI, 2007)

In terms of information management, confidentiality and integrity practices are critical in order to ensure that information is protected from unauthorised access or misuse (ITGI, 2007). Ensuring the authenticity of information is also essential to improving organisational decision making and planning (ITGI, 2007).

In terms of systems and services metrics related to availability and reliability are essential for an effective control framework as they ensure operational continuity and ensure that the system is able to deliver the information even during peak operational periods (ITGI, 2007). Finally organisations need to adopt a audit program that ensures compliance with the legal aspect of service delivery and ensuring that all service level agreements and contracts are adhered to.

The main purpose of the COBIT framework is focussed on defining best practice processes that allow IT service delivery to be assessed and monitored (Simonsson and Johnson, 2006). Furthermore Simonsson and Johnson (2006) believe that the real value of COBIT can be seen in the strategic impact of IT to the business by mapping the top level assignments and responsibilities to the appropriate resources.

Hawkins, Alhajjaj and Kelly (2003) argue that the COBIT framework is a systems model that needs to be adhered to in order for governance to be implemented successfully in an organisation. Hawkins, Alhajjaj and Kelly (2003) assert that governance starts with managers developing a strategic plan for the organisational IT environment. The next stage is to identify reliable service providers and develop and draw up the terms of engagement for service providers. These terms of engagement are defined by COBIT as the acquisition and implementation phase of COBIT.

Once the appropriate service provider has been identified the next step will be to determine whether the policies and plans defined by the board are effective in delivering service to the business (Hawkins, Alhajjaj and Kelly, 2003) During the monitoring phase corrective action needs to be taken for any plan that is not achieving its goals (Hawkins, Alhajjaj and Kelly, 2003). According to Hawkins, Alhajjaj and Kelly (2003) when following this COBIT process organisations are able to focus attention on areas of the organisation that are vulnerable and reduce the risk of failure in these areas.

In addition to COBIT the Sarbanes-Oxley Act also provided business with a blueprint to implement effective IT control in the organisation. The Sarbanes-Oxley Act was instituted in the Unites States in 2002. In terms of section 404 of this act, organisations are required to ensure that systems used in the organisation to process and store data are effective at providing reliable information to the shareholders (ITGI, 2004). In addition this act made it mandatory for organisations to implement

effective governance models which would provide them with a framework in which to operate and identify material weaknesses within the systems.

In terms of this act various controls had to be implemented at each level of the organisation. Executive management were tasked with establishing an IT strategic plan that incorporated the organisational business activities. This plan entailed setting business objectives and policies and ensuring that decisions are made on how to deploy and manage the resources of the organisation. The plans and policies are then communicated throughout the organisation (ITGI, 2004). The organisational strategies then had to be transformed into business processes which are the mechanisms the organisation uses for creating and delivering value to its stakeholders (ITGI, 2004).

Another key outcome of this act was that it resulted in organisations taking risk analysis more seriously. Management were now more involved in the identification and analysis of risks that impacted on the objectives of the organisation. Management also ensured that controls were implemented to ensure that personnel were able to mitigate against the risk of their project prior to approval as well as during the implementation phase (ITGI, 2004). In addition to risk assessment, organisations were now also responsible for assessing the impact of the risk on the organisation as well as the probability of the risk occurring. Oettinger and Legates (2000) contends that the risk of any IT investment decision needs to be weighed up against potential strategic value that they can deliver to the organisation.

According to Damianides (2005) one of the unintended consequences of the growth of IT is that new threats are always pervasive in the cyber age especially for strategic information that is stored, transmitted and retrieve through electronic processes. As part of the governance and control processes required by SOX organisations needed to ensure that “information is protected against harm from vulnerabilities such as loss, inaccessibility, alteration and wrongful disclosure whether they are caused by errors, omissions, fraud, accidents or intentional damage” (p 83, Damianides, 2004)

In terms of data management South African organisations are currently compelled to adhere to the provisions of the electronic communications and transactions act 25 of 2002. According Michalsons (2008) the promulgation of this act has created a formal framework for the development and governing of electronic transactions in South Africa. This act according to Michalsons (2008) ensures that organisations now need to be more conscious of their efforts to manage information as it gives legal recognition to electronic contracts.

Michalsons (2008) also argues that the impact of the widespread use of electronic documents requires a paradigm shift in the management and storage of information. Michalsons (2008) contends that the influence of the act will impact upon business processes as organisations consider what the primary format of transactions and informational records are. The result of this is that organisations need to review information management approaches as the act now recognises data messages as "writing". Data messages therefore can now be used as evidentiary proof (Marx, 2003).

Cliff Dekker (2008) endorses the views of Michalsons (2008) as they state that the act gives new weight to the legality of electronic documents which may be regarded as an original where its integrity is assured. According to Cliff Dekker (2008) the act also now requires business to ensure the confidentiality and protection of information as organisations need to stipulate their security procedures and privacy policy in respect of personal information when conducting business over electronic mediums as any breach of these stipulations could result in penalties for the service provider.

In addition the King II report of 2001, which provides organisations with a set of best practices for corporate governance, addresses the issue of the role of IT for South African organisations (King, 2001). According to this report, management needs to understand the risks and challenges associated with technology so that that they are able to discharge there duties effectively (King, 2001).

According to King (2001) the areas that are most impacted by IT are internal control systems, where management should ensure that business controls are integrated into the systems. It is the responsibility of management to ensure that these controls are adhered to. The King recommendation also emphasises that reporting based on IT systems should be accurate and the authenticity of information should not be compromised. Furthermore according to King (2001) if information is made

available through electronic channels the organisation should ensure that all stakeholders have access to this information.

In terms of an executives fiduciary duties, organisations need to take into account the impact of intellectual property rights when using IT (King, 2001). King (2001) also argues that the use of IT also has implications for business in terms of:

- Admissibility of electronic evidence;
- authenticity and integrity of electronic communications;
- verification of dispatch and acknowledgement of receipt; and
- management and retention of records

The King report (2001) also reviews management's role in the valuation of IT especially as it relates to IT Strategy. King (2001) believes that adopting value management practices are critical due to the constant innovation and development that exists in this area as it makes decisions on IT expenditure particularly important. King (2001) argues that traditional value management principles are not applied in this area as technology expenditure is based on instinct and not on commercial principles. According to King (2001) the valuation of technology needs to be reviewed and organisations need to implement economic evaluation criteria in order for the interests of the stakeholders to be honoured. Due to the critical nature of IT on the business processes of an organisation, the King report also recommends that management needs to ensure that necessary skills are in place to ensure that the organisation effectively implement their of internal control systems (King, 2001).

In the public sector, departments and institutions are required to adhere to the Public Finance Management Act (PFMA), 1999 (Act No. 1 of 1999) (as amended by Act No. 29 of 1999), this act, promotes the objective of good financial management and provides public organs with guidelines in terms of the management and reporting of financial information (Setsoto, 2008).

According to Setsoto (2008) the main objectives of the act is to ensure that there is more accountability in terms on the control and management of financial information and to improve the accuracy and validity of information. The act also wishes to ensure that there is transparency in terms of the

operation and control of government expenditure and borrowings (Setsoto, 2008) The act also ensures that the flow of information between the treasury and the various departments is improved.

In addition to the PFMA the government also introduced the Local Government Municipal Finance Management Act, Act Nr. 56 of 2003. The objective of this act is to ensure that local authorities and municipalities maintain a management accounting and information system that accounts for the assets and liabilities of the municipality (Kotane, 2008).

The Access to Information Act of 2000, protects the constitutional right to access information under the control of the government. This act provides for citizens to gain access to information while ensuring a reasonable protection of privacy, commercial confidentiality and effective, efficient and good governance. The objective of this act is to ensure that citizens of South Africa have access to information from public or private bodies upon compliance with the requirements of the act.

According to the act, the government information officers are responsible for ensuring that information that is held in electronic format should be available for access to citizens but without impacting on the integrity and confidentiality of the government information systems (Kotane, 2008). The challenge for government Information officers is therefore to ensure that they are able to protect the assets of the government but still provide access to information without too much complication. Additionally information officers should ensure that information that could jeopardise the security or defence of South Africa is not accessible for public consumption (Kotane, 2008).

In addition to these acts government information systems also needs to comply with the guidelines that have been outlined in the Minimum Interoperability Standards framework (MIOS) of 2007. The objective of this framework is to provide government institutions with guidelines for the implementation of information systems that will enable them to build value added information and services. In terms of the MIOS, departments are responsible for improving the business processes in line with the structured approached provided by the MIOS framework. The aim of the MIOS is to provide government departments with consistent policies, principles and standards which will ensure that government information systems are transformed in a manner that will improve service delivery (MIOS, 2007)

According to MIOS the government strategy is for all departments to collaborate and share information in order to improve citizen service delivery. National, provincial and local government departments are all required to work across their boundaries in order to ensure that information and services are effectively delivered to business and to citizens (MIOS, 2007).

Through adopting the MIOS framework, government believes that it will improve the capability of departments to confidently manage, transfer and exchange information and services (MIOS, 2007). The principles, guidelines, and standards enshrined in this framework should underpin sound management, and establish concepts, practices and tools that will drive the successful sharing of services across government boundaries." (MIOS, 2007, p3)

2.8. Literature Conclusion

The review of the literature has shown that IT systems and services need to add value to the business. In order to achieve this, organisations need to ensure that they implement the necessary structure and processes to manage the IT environment so that the business is able to achieve their goals. In order to ensure that this framework is in place, senior executives in the organisation need to show their commitment to governance initiatives by driving awareness and support for a formal governance framework.

The structure of the IT Governance organisation is also critical as it is concerned with the manner in which decisions are made in the business. The responsibility and accountability of the various personnel involved in IT Governance, and the manner in which the IT organisation engages with the business are the key areas that need to be addressed in the organisation. In this context decision making relates to both the technological and business imperatives of the organisation and the business processes that the IT systems support. The structure of the decision making framework in the organisation is critical to a successful IT Governance configuration as it ensures that IT understands the needs of the business and is able to apply a standard process across all projects in the planning, design, implementation and support of all systems in the organisation.

The literature on business-IT alignment has focussed mainly on the need to ensure that the systems which support the business strategy and operational processes in the organisation are representative of the functional requirements of the business, from a governance perspective IT need to ensure that they are able to adapt to the needs of the organisation in the competitive environment. In the current environment, organisations need to ensure that their systems are integrated in the operational fabric of the business in a manner that ensures they provide the business with an advantage. The alignment of IT systems needs to span across applications, communication systems and professional services. The objective of the alignment between IT and business is to ensure that information is available and accessible on any platform while ensuring accuracy of the data.

The literature has also highlighted two outcomes which organisations that embark on IT Governance initiatives are concerned with. Governance, should be concerned with increasing the value of the organisation while managing the risk that the organisation is exposed to. In terms of value, organisations

are mainly concerned with ensuring that the investment which they have made in IT assets provides a benefit to the organisation either in terms of productivity gains which ensure an improved financial benefit or in terms of operational effectiveness. In order to ensure that value is generated from IT, it is critical that a framework is adopted to manage and measure the performance of IT systems in the organisation and their contribution to the business performance.

In terms of risk management organisations need to ensure that they are aware of both their legal obligations and the operational practices that ensure that information is protected. In a legal context, organisations need to understand the responsibility which legislation places upon them in terms of contractual and national law. In addition to this financial reporting standards have become stricter and the management of information in these systems now also need to comply with both industry regulations and global standards. The control and access to information has also become an important factor in the risk management practices of the organisation as they need to ensure the confidentiality and integrity of the information.

2.9. Research Questions

Based on the literature reviewed the following questions have been derived and will be investigated.

Question 1

What have been the major drivers for ensuring that business and IT are aligned in the public sector?

Question 2

How is the value that is generated from IT within the public environment defined and measured?

Question 3

What are the key components of the IT risk management program within the public sector?

Question 4

How is the performance of IT within the government assessed?

Chapter 3

3. Research Methodology

In order to select the most appropriate methodology and research instrument to utilise during this study it was critical to ensure that the researcher adopted an approach that looked at the characteristics of the processes, as well as gain an understanding into the generation of IT value and governance in the public sector. Understanding the factors that influence governance would ensure that the research has a degree of practical relevance (Galliers and Land, 1987). In choosing a research methodology Miller and Dingwall (1997) believes that the researcher needs to understand how the methodology will help in the analysis and explanation of the phenomenon which he is studying. According to Creswell (2003) the research framework has to support the specific question which the research is trying to address and has to cover procedures about data collection, analysis and reporting.

In order to comply with the principles set out by Creswell (2003) it was decided to adopt the cognitive mapping approach to analyse the information gathered from the various sources. According to Ahmad and Ali (2003), this technique will allow the researcher to conduct a process which is logical, systematic and concerned with seeking solutions to problems and answering research questions.

The mapping study is typical of a qualitative research framework where the focus is on understanding a particular phenomenon. The researcher's use of a qualitative approach is supported by Ahmad and Ali (2003) since this research is concerned with describing rather than explaining the relationship between variables and coming to terms with the meaning, not the frequency, of the phenomena. Ahmad and Ali (2003) further argue that this approach will allow the researcher to gain an understanding of how things happen and how they are related, rather than only measuring the relationship between variables.

The cognitive maps enabled the researcher to develop a holistic picture of the main themes and concepts related to IT value and governance, and advance a framework for its understanding. The utilisation of cognitive mapping allowed the researcher to also identify the properties and characteristics which existed within the domain of IT Value and governance in the public sector. Through the use of this technique the researcher was able to develop a scheme which represents the knowledge

of the interviewees. The cognitive mapping approach also ensured that the researcher was able to assess the cause-effect relationship between events, activities and processes as well as the dependencies on these processes.

Miller and Riechert (2004) point to the fact that cognitive maps have their origin in constructivism. This allowed the researcher to utilise the information gathered from the literature reviews to asses the data gathered from the interviews to generate an assessment of the state of IT value and governance in the South African public sector. This argument is carried forward by Mayring (2000) who states that this process allows the researcher to work with knowledge that was formulated prior to the research and develop the main categories into which information can be placed based on the answers of the responders.

Since issues surrounding value generation and governance are multifaceted and differing points of view are available on the topic the cognitive mapping approach prevented the researcher from presupposing the importance of certain activities within IT Governance. Due to the fact that various organisations participated in this research and individuals who fulfil different roles within these institutions were interviewed, the use of cognitive mapping to assess stakeholder perceptions allowed the researcher to address complex topics that included numerous issues and diverse points of view as Jackson and Trochim (2002).

3.1. Research design

The approach adopted by the researcher is what Creswell (2003) views as constructivist. This framework aims to gather information from multiple sources with different points of view in order to generate an understanding of the phenomenon. The constructive approach according to Creswell (2003) is based on the notion that researchers seek to gain an understanding of a subject based on the subjective experiences of respondents. Creswell (2003) argues that because these views are diverse the researcher needs to ensure that when pressing for information he ensures that his questions are broad and general in order for respondents to construct there own meaning of a situation. According to Creswell (2003) constructivists also focus on specific contexts in which people live and work in order to understand what influences a person's point of view. It was therefore necessary for the researcher to personally be in the environment of the respondent to understand the perspectives that have shaped his opinions (Creswell, 2003).

An interview framework for this research was used to gain an understanding of the characteristics and dynamics that are involved in public sector IT initiatives. Through the use of this methodology the researcher was able to gather the opinions of various stakeholders. The interview methodology also allowed the researcher to understand the dynamics of IT Governance and examine the interaction between business and IT (Pinsonneault and Kraemer, 2006).

3.2. Population and Sampling

In order to get a better understanding of the elements that influence the research the researcher gathered information from various role players. A purposive sampling technique was adopted as it allowed the researcher to obtain views from various organisations. In determining the sample the researcher placed an emphasis on people that have had experience in either the management or control of IT. The sample included various executives, managers, governance practitioners and professionals who are involved in the planning, development and control of IT within the public sector. The Sample included organisational Chief Information Officers (CIO), departmental deputy directors; senior managers involved in governance and IT management.

This study examined the practices and views of IT value and governance within the Public Sector. The public sector organisations that participated in this research included government organisations at the national, provincial and local level as well as parastatals and state owned entities that provide critical information and financial services to the government

According to Brink (2001) the use of purposive sampling is justified when the views and opinions of specialists and experts are required. However Brink (2001) also warns against the limitations of purposive sampling which include:

- Potential for sampling bias;
- Use of a sample that does not represent the population; and
- Very limited generalisation of the results;

The researcher was cognisant of these limitations and had therefore attempted to control the influence of these factors. Firstly in order to avoid bias the researcher gathered information from various organisations and sources to ensure that multiple perspectives were examined. In the event that respondents had different viewpoints on the subject the researcher has highlighted these. The researcher ensured that the sample that had been identified were knowledgeable on the current practices of the subject within their industry.

3.3. Data Collection

Data collection for this research was accomplished through conducting semi-structured interviews with open ended questions. The formats of the interviews that the researcher undertook were face-to-face. Lists of the guiding questions are presented in appendix C. These questions were used to stimulate the discussion.

According to Miller and Dingwall (1997), the utilisation of interviews for data collections is interpretive in nature and is conducive for qualitative research due to the fact that it is effective in constructing relationships between researchers and the people that they study. Miller and Dingwall (1997) also believe that through the use of interviews the researcher is able to asses the feelings and believes of a respondent as well as gather valuable information based on the experiences of the respondent. The interview approach allowed the researcher to also place the views of the respondent within the greater context of the literature on the subject (Miller and Dingwall, 1997).

The benefits of the interview technique according to Creswell (2003) are that it allows the researcher to control the flow and direction of the interview based on the line of questioning. Creswell (2003) also believes that interviews are the most appropriate technique to gather data that is dependant on personal experience and knowledge. The adoption of this approach allowed the researcher to intervene and provide clarity and guidance to the researcher when concepts were no fully understood.

During the interview process the researcher utilised the framework proposed by Ackermann, Eden and Cropper (1992). During the initial stage the researcher attempted to engage the respondent in order to understand the role of IT in their organisations.

The next stage of the engagement with the respondent allowed the researcher to ask the respondents to identify which concepts were related and describe the nature of the relationships. Finally the researcher asked the respondent to define specific processes which related to IT value and risk management. During the interview session the researcher recorded the discussion which was then transcribed to check and confirm the data.

3.4. Data analysis

The approach to analysis adopted for this research was based on cognitive mapping analysis. Through the use of this technique the researcher ensured that all views on a particular theme were considered (Kelle, 1998). The occurrence of similar views also allowed the researcher to determine the strength of a particular point of view. Through this technique the researcher was able ensure that the analysis was reliable as similar rules and procedures were followed for each respondent. The utilisation of cognitive mapping for this research, allowed the researcher to explore the commonalities and individualities in the responses from the various interviewees (Tyler, 2001).

The first stage of developing the maps was to ensure an accurate representation of the statements in the map and links those statements that need to be linked together in order to get a clearer picture of the relationship between the statements and to see where there are similarities and differences between the views of the different stakeholders. The outcome of this stage was a holistic picture of the governance domain which was assessed.

The researcher firstly constructed a map for each respondent which was then used to determine which statements were linked to the specific areas under review, and which statements were isolated. The next step was then to categorise statements into groups based on the concepts that they described and the relationship and processes that they explained. The researcher was then able to identify the dominant themes that are present within IT Governance and control structures. Finally the researcher was able to link back the finding of the data collection process to the literature and research questions in order to adopt a position on the IT Value and governance in the public sector.

3.5. Validity and reliability

The validation of this report covers both how effectively the instrument measured what it purported to be measuring, as well as whether the research covers content of the field of study. Reliability addressed the issue of how accurate the research instrument was.

According to Creswell (2003) validity in qualitative research is not the same as that in quantitative research. Creswell (2003) argues that qualitative researchers need to ensure that consistent themes are developed across respondents.

3.5.1. Internal validity

Miller and Dingwall (1997) argue that the validation of social science research cannot be achieved by the replication of the situation but through the judgement of the peers and experts who can recognise and understand the information that has been presented on the subject.

The researcher has therefore ensured that the study is internally valid by evaluating the conclusions drawn from the analysis through the process of peer reviewing (Creswell, 2003). This process Creswell (2003) asserts involved locating a subject matter expert who debriefed the researcher on his findings, by asking questions about the conclusions drawn by the researcher to ensure that the research resonated with people other than the researcher.

3.5.2. Content Validity

Dahlberg and Kivijärvi (2006) contend that content validity refers to how accurately the measurement instrument that was being used can represent the domain of knowledge that was being investigated. The content validity of an instrument can only be determined by assessing whether or not the instrument is able to achieve its purpose in gathering information about IT Governance. Therefore, the domain of interest was clearly defined. In the case of IT Governance, each definition validated to ensure that it was consistent within the IT Governance field (Dahlberg and Kivijärvi, 2006).

The researcher has used subject matter experts in order to determine whether or not the themes being developed were appropriate in the context of IT Governance in order to determine their relevance and representativeness to the content domain.

3.5.3. External validity

As the focus of this study is predominantly qualitative we are more concerned about identifying the unique characteristic of the governance process (Powell, 2006) and less so about being able to generalise the results across the population.

3.5.4. Reliability

The researcher focused on two areas of reliability identified by Krippendorf (1980), stability and consistency. In order to ensure that the analysis of all the data was consistent, the researcher limited the amount of time taken to analyse all the transcripts and ensured that it was all done within a period of no more that two weeks therefore preventing the researcher from interpreting data differently at different times. In order to ensure that this study could be replicated the researcher has endeavoured to follow a structured and documented assessment protocol and utilised processes from previous studies in IT management that are relevant to this topic.

Chapter 4

4. Research results

The development of the cognitive maps aimed to retain as much of the direct account from the interviewees as possible (Ackermann and Cropper, 1992). Each part of the map represents distinct elements that were discussed during the interview process and are connected in order to provide an overview of the entire value creation and governance processes that are undertaken by the institutions. The model is constructed based on the central idea of public value and the related governance domains which were then separated into subcomponents based on the practices and plans that were discussed during the interview process.

In order to determine the key issues, an analysis was undertaken which allowed the researcher to look at all the concepts and the interrelationship between these elements in order to understand the practices within a specific domain (Ozen sand Ulengin, 2001). The phrases within the maps themselves are all fundamental components of the body of knowledge collected during this process. In order to ensure that information was represented accurately, all concepts that were addressed by multiple respondents were not removed as they may have lead to alternative actions or finding at the next level in the map.

4.1. Cognitive Maps

Figure 5: Cognitive Map for Interview 1

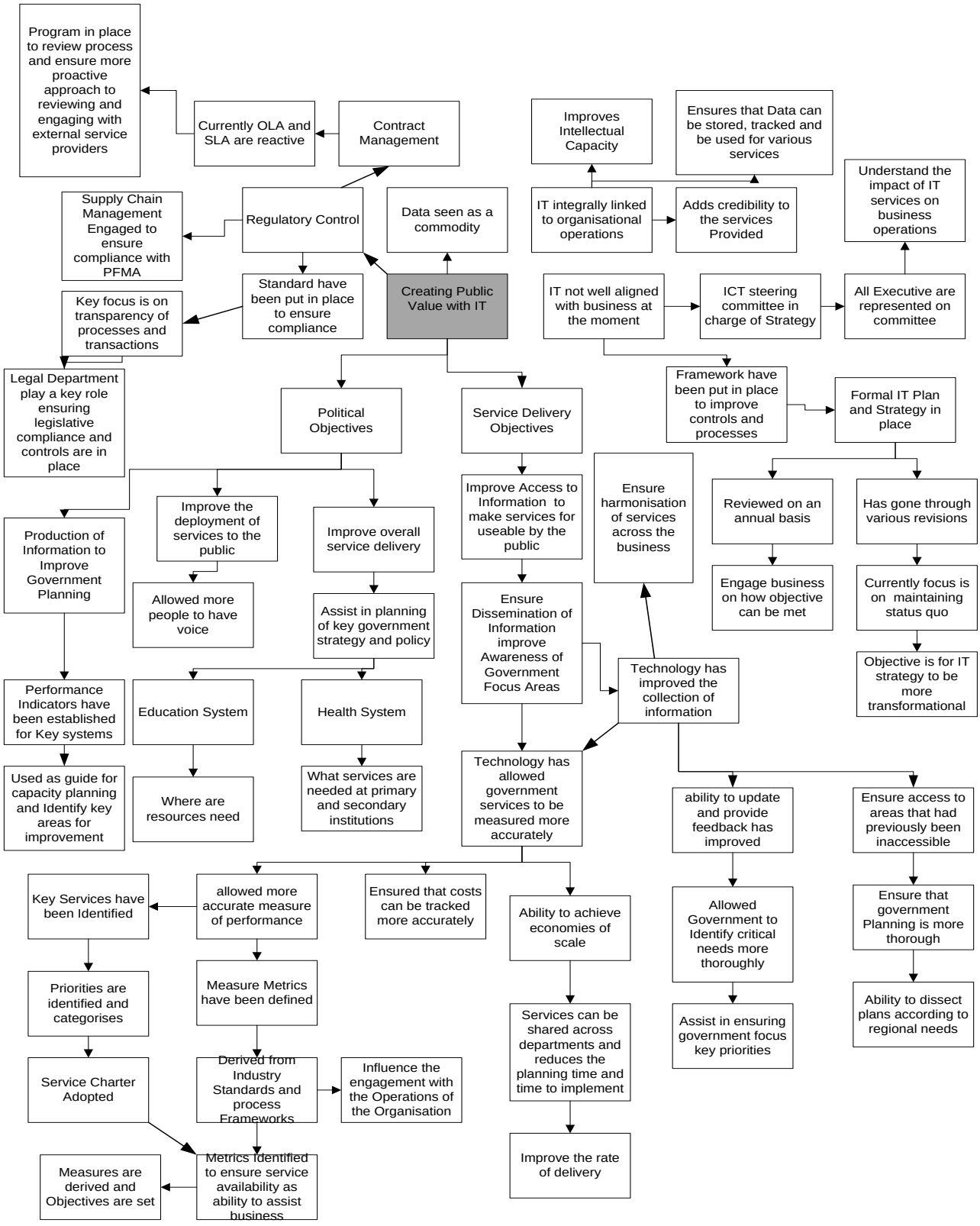


Figure 6: Cognitive Map for Interview 2

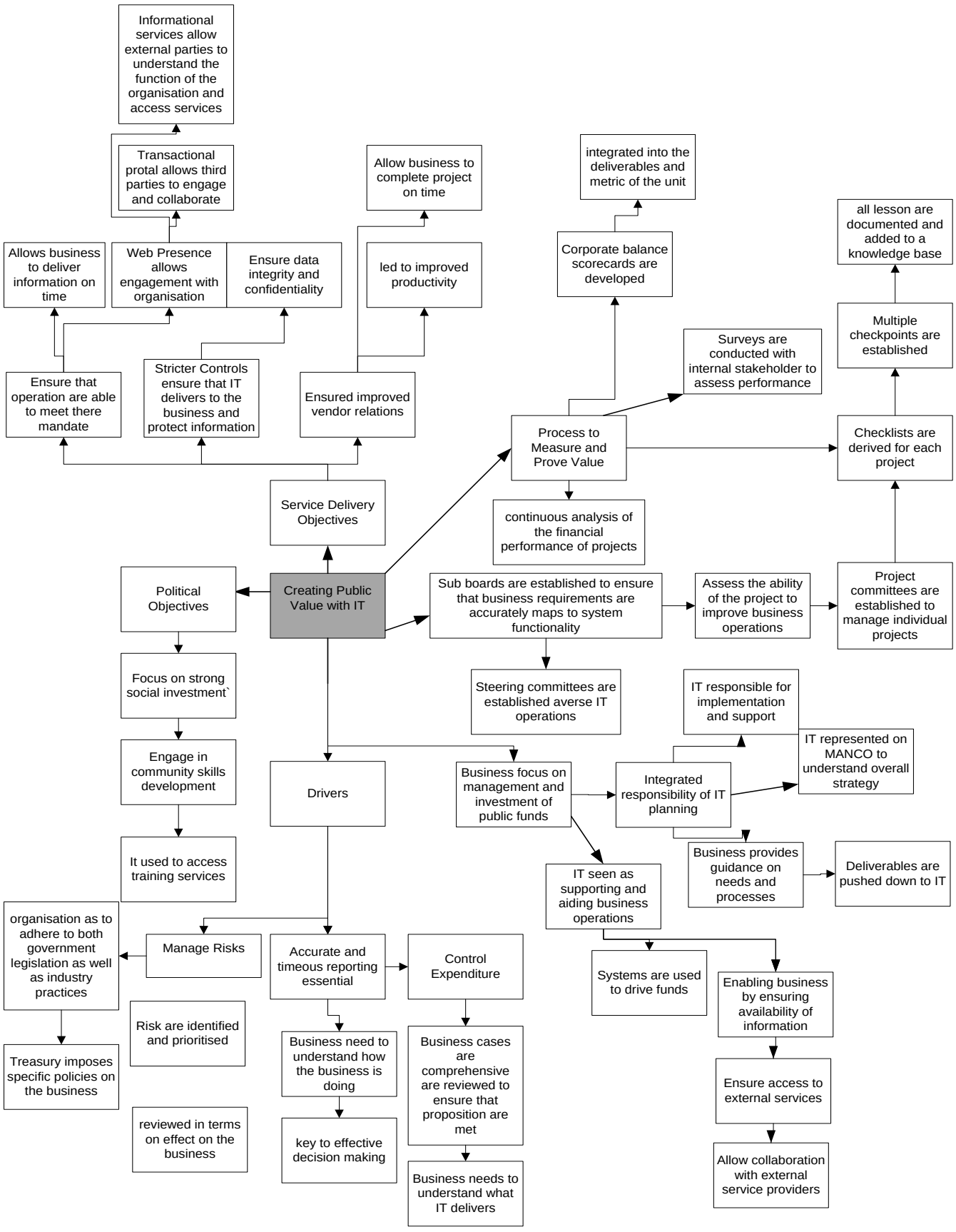


Figure 7: Cognitive Map for Interview 3

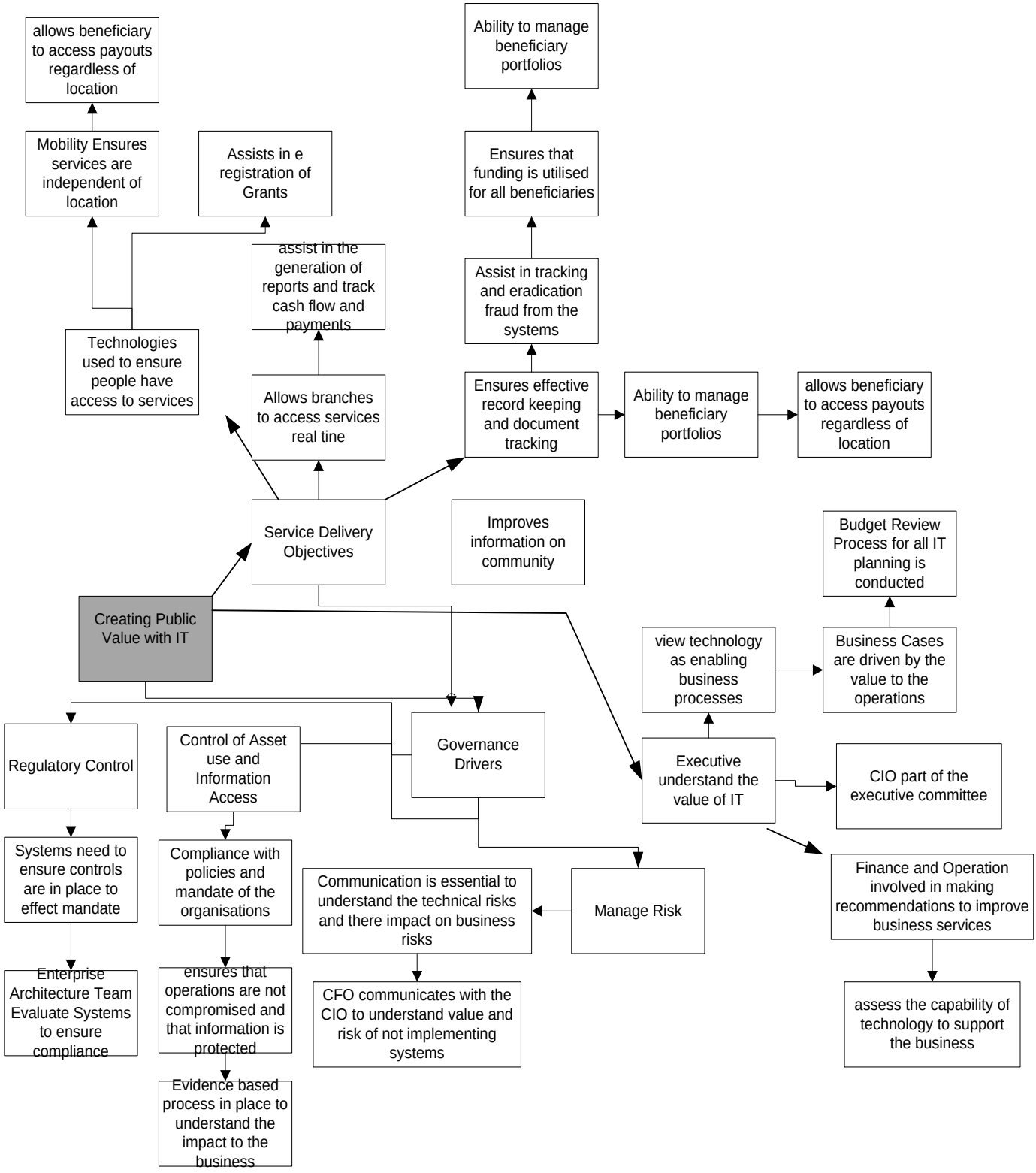


Figure 8: Cognitive Map for Interview 4

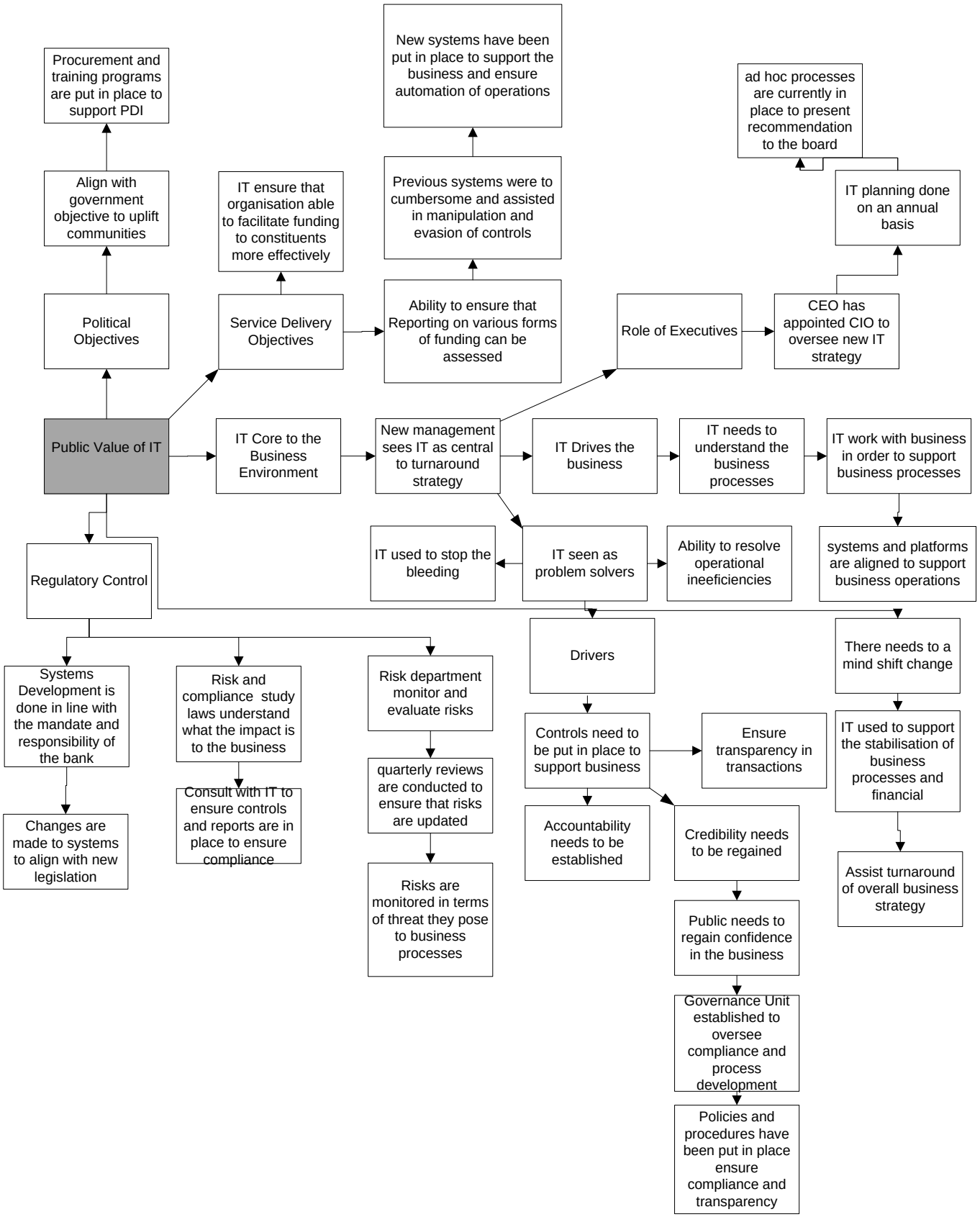


Figure 9: Cognitive Map for Interview 5

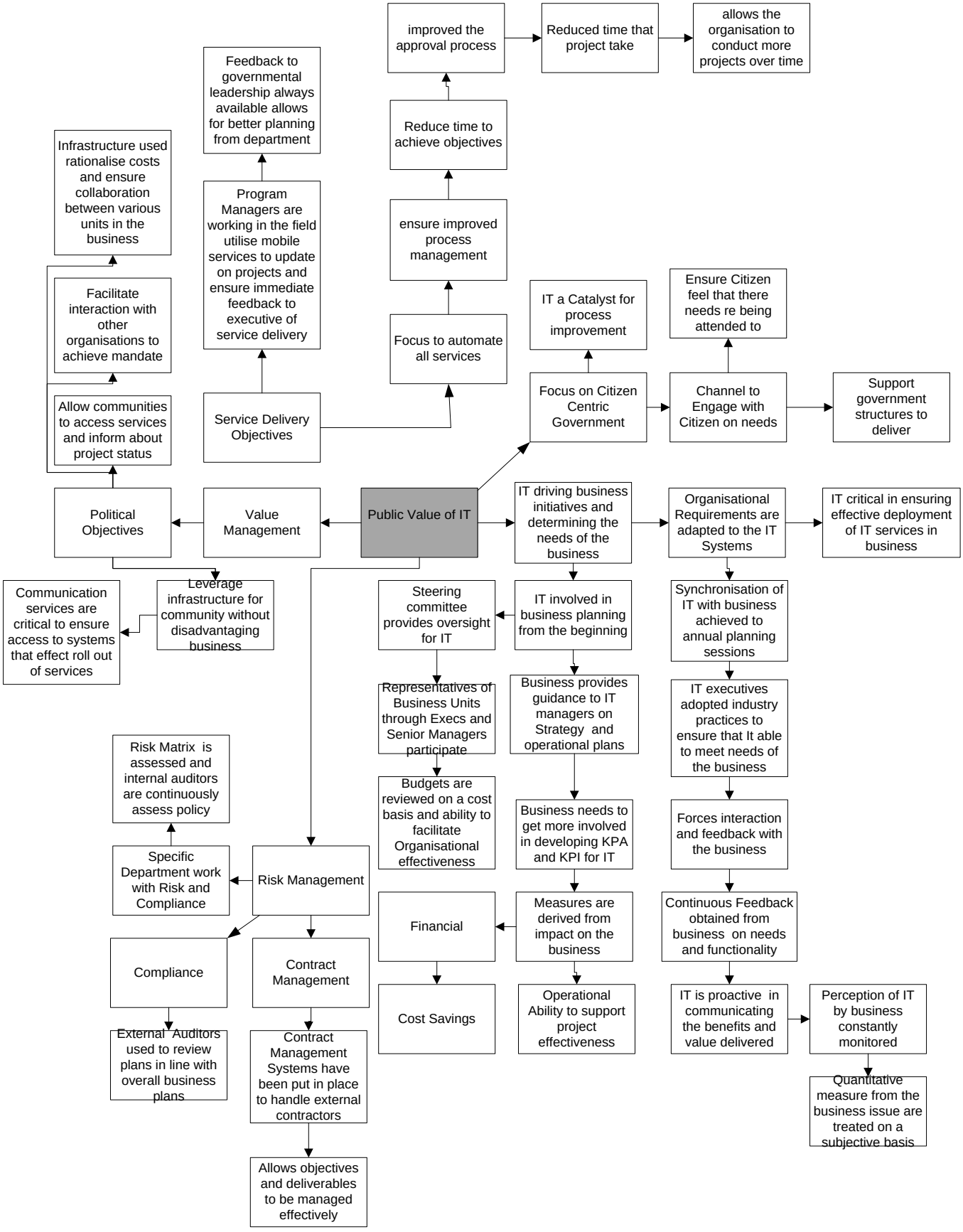


Figure 10: Cognitive Map for Interview 6

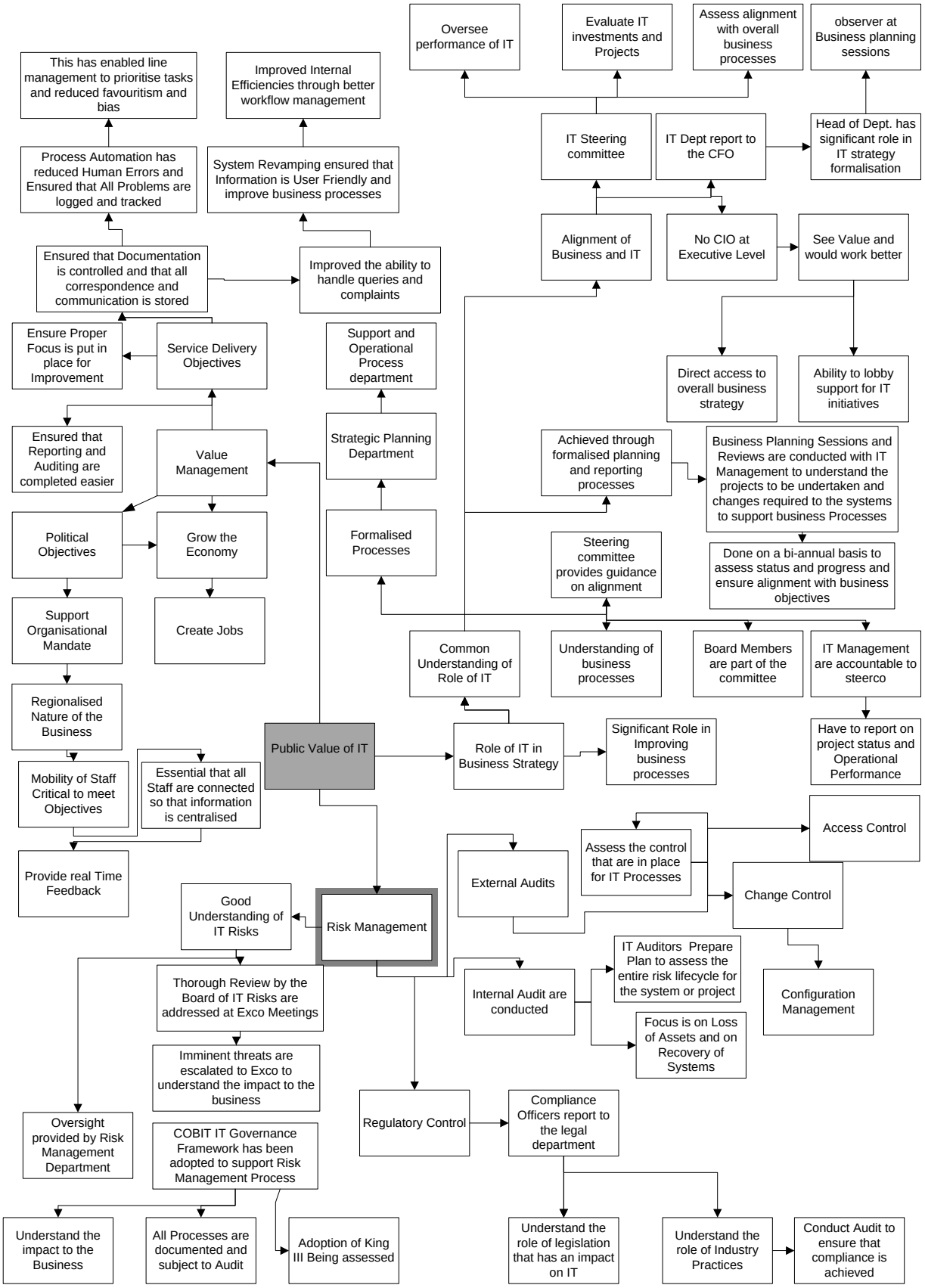


Figure 11 : Cognitive Map for Interview 7

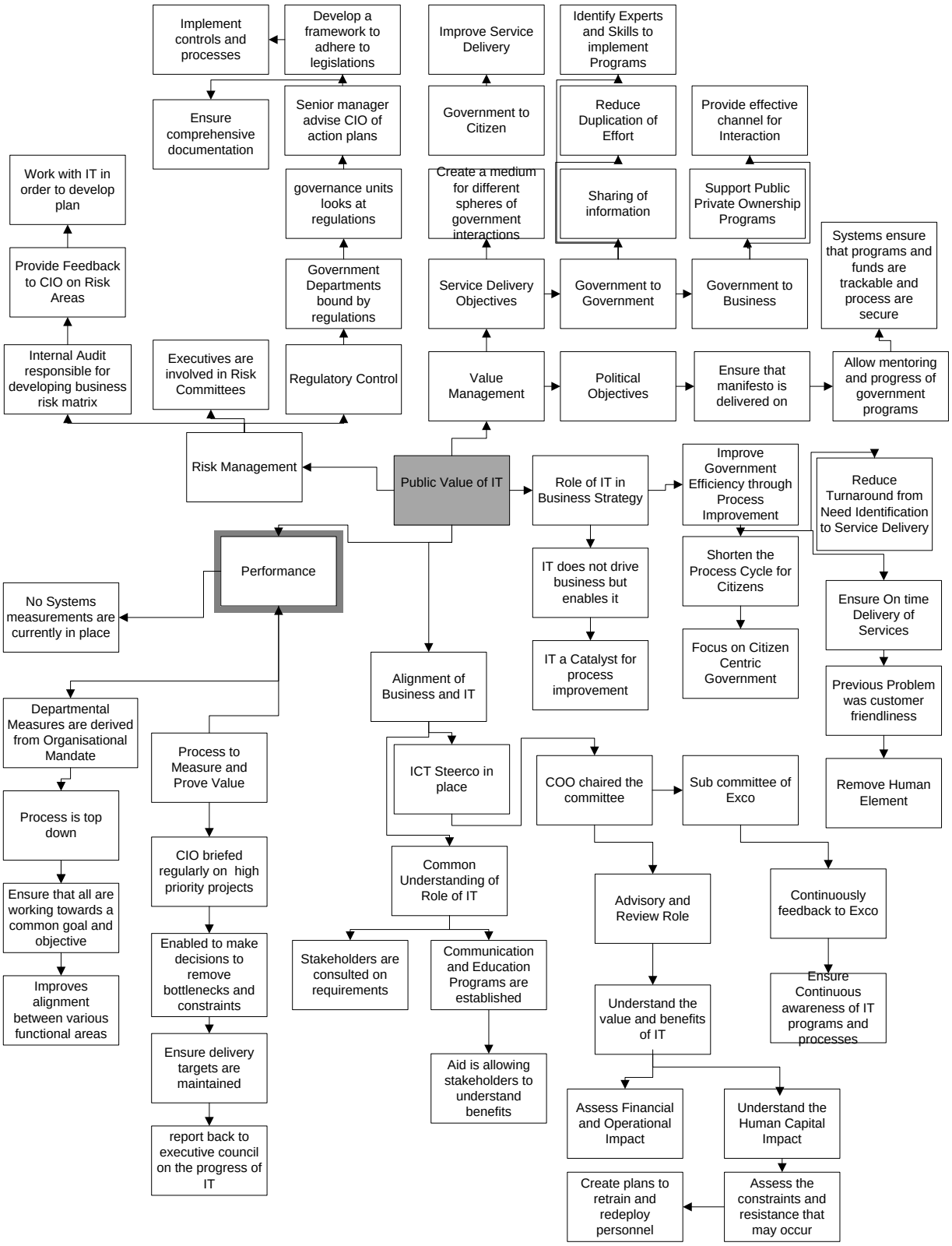


Figure 12: Cognitive Map for Interview 8

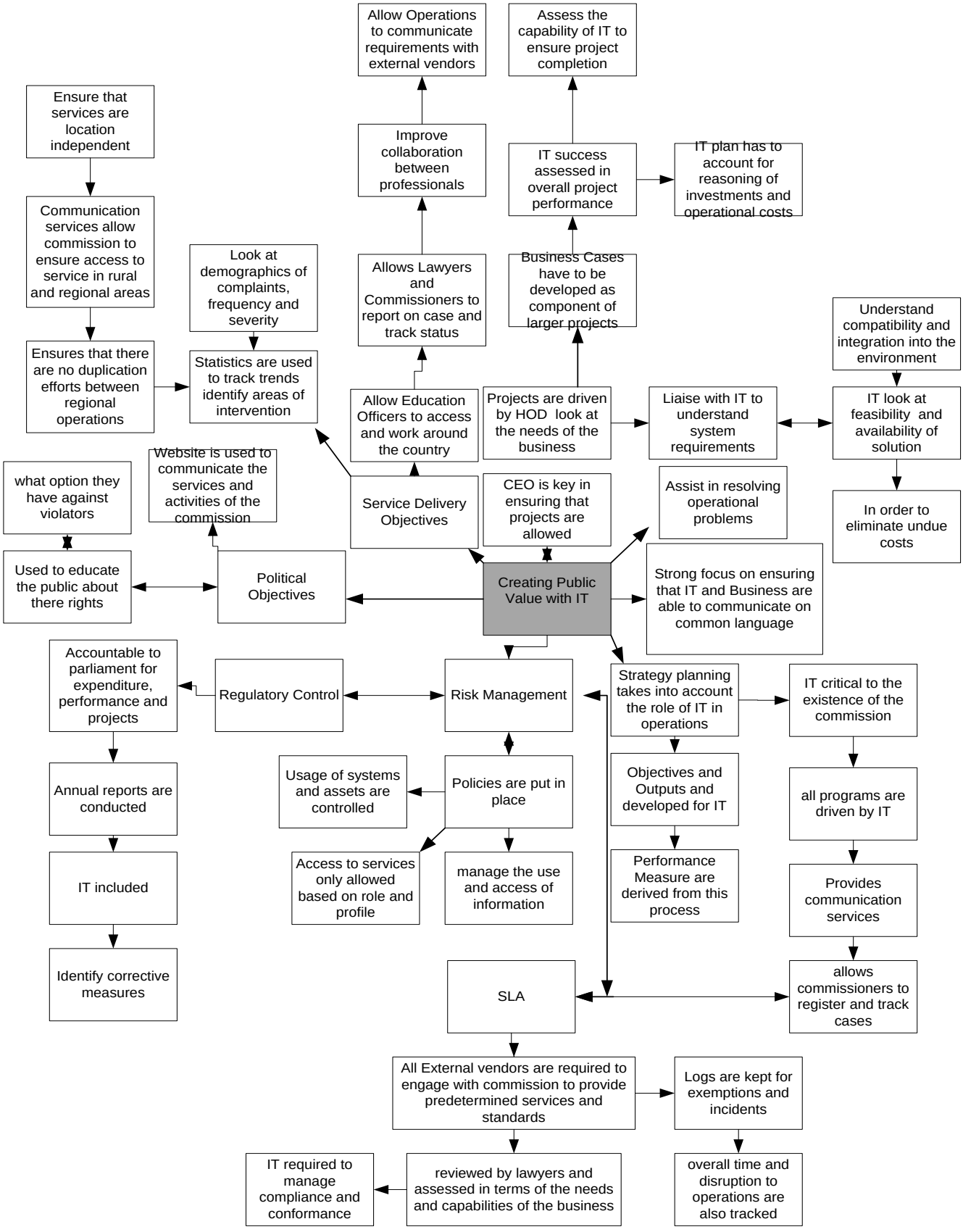


Figure 13: Cognitive Map for Interview 9

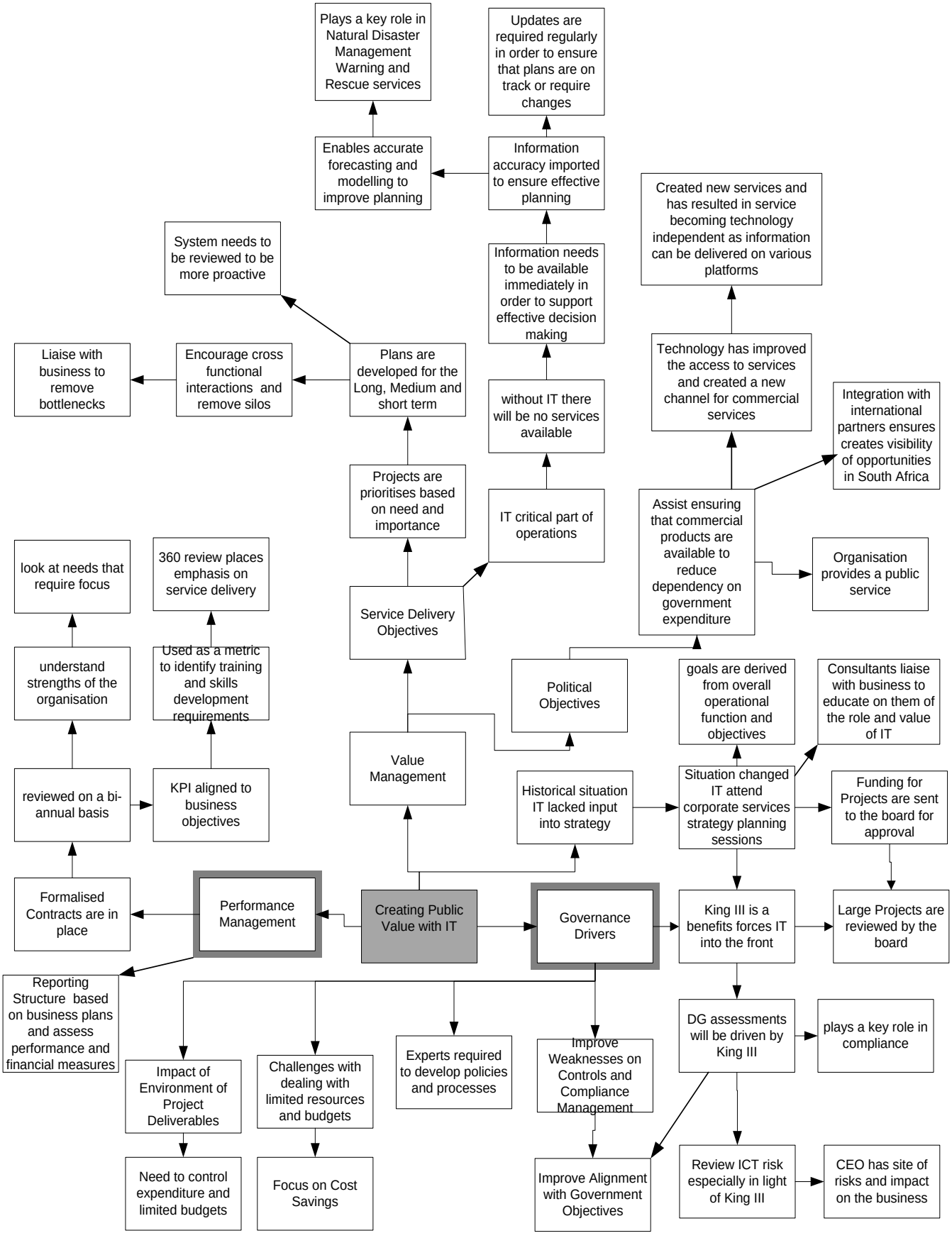


Figure 14: Cognitive Map for Interview 10

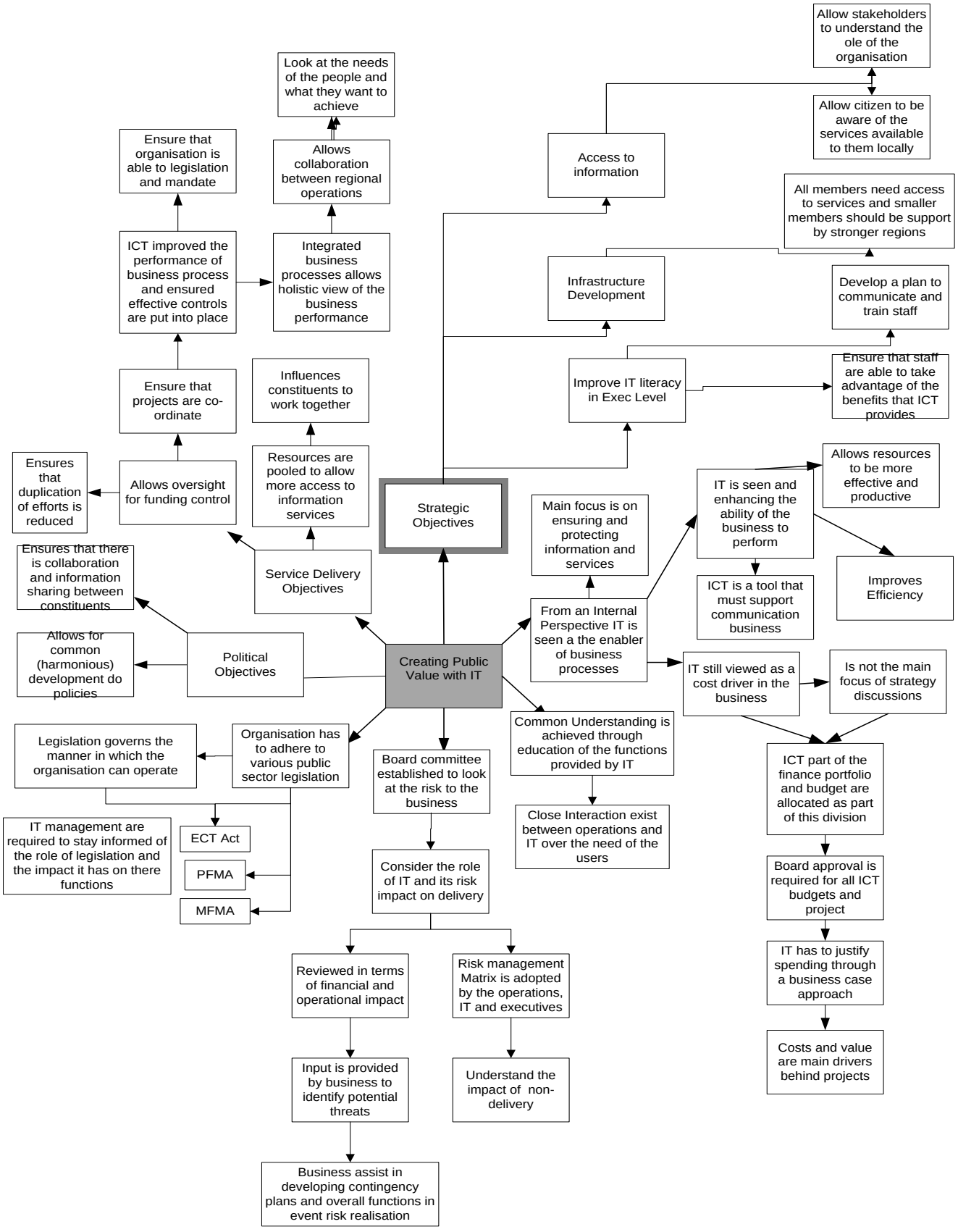


Figure1 5: Cognitive Map for Interview 11

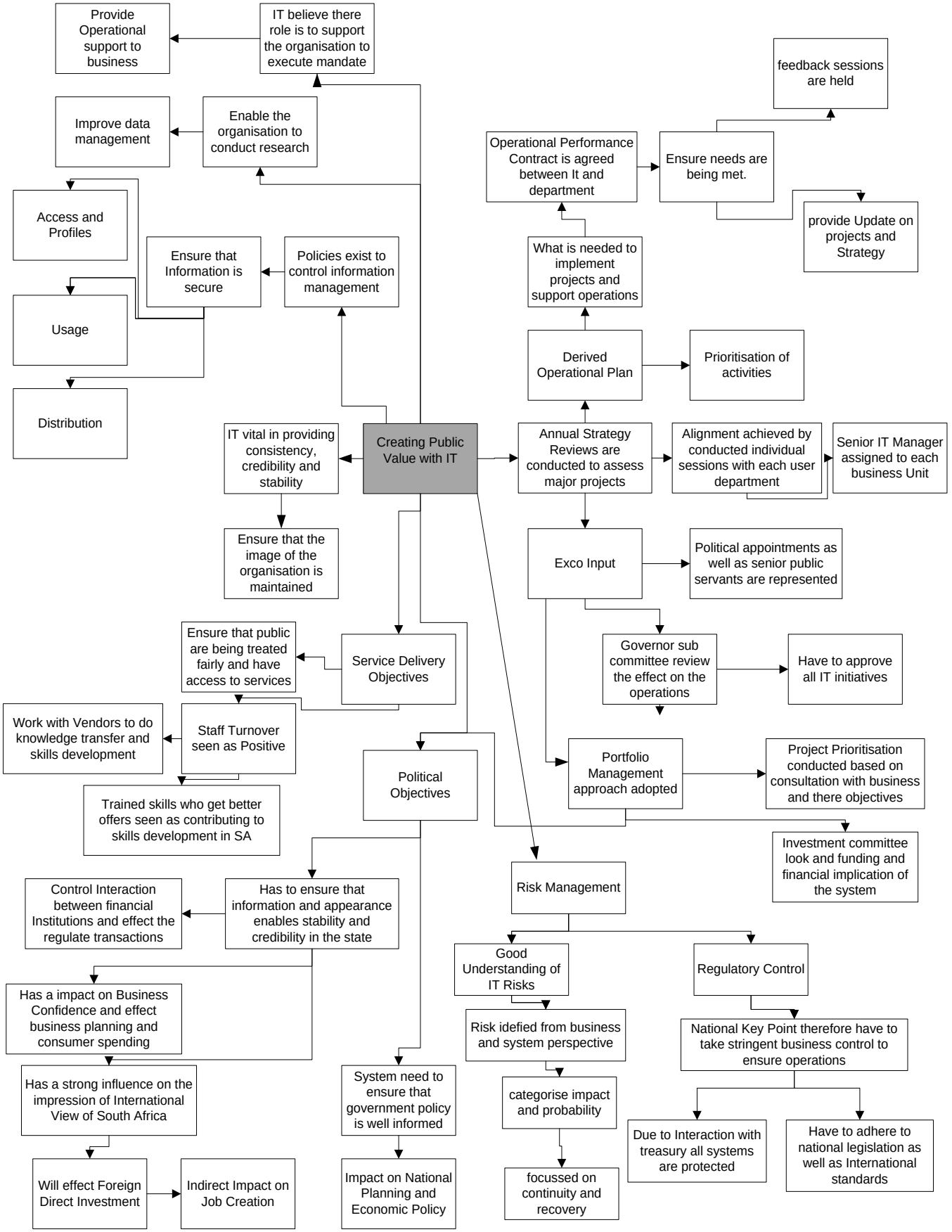


Figure 16: Cognitive Map for Interview 12

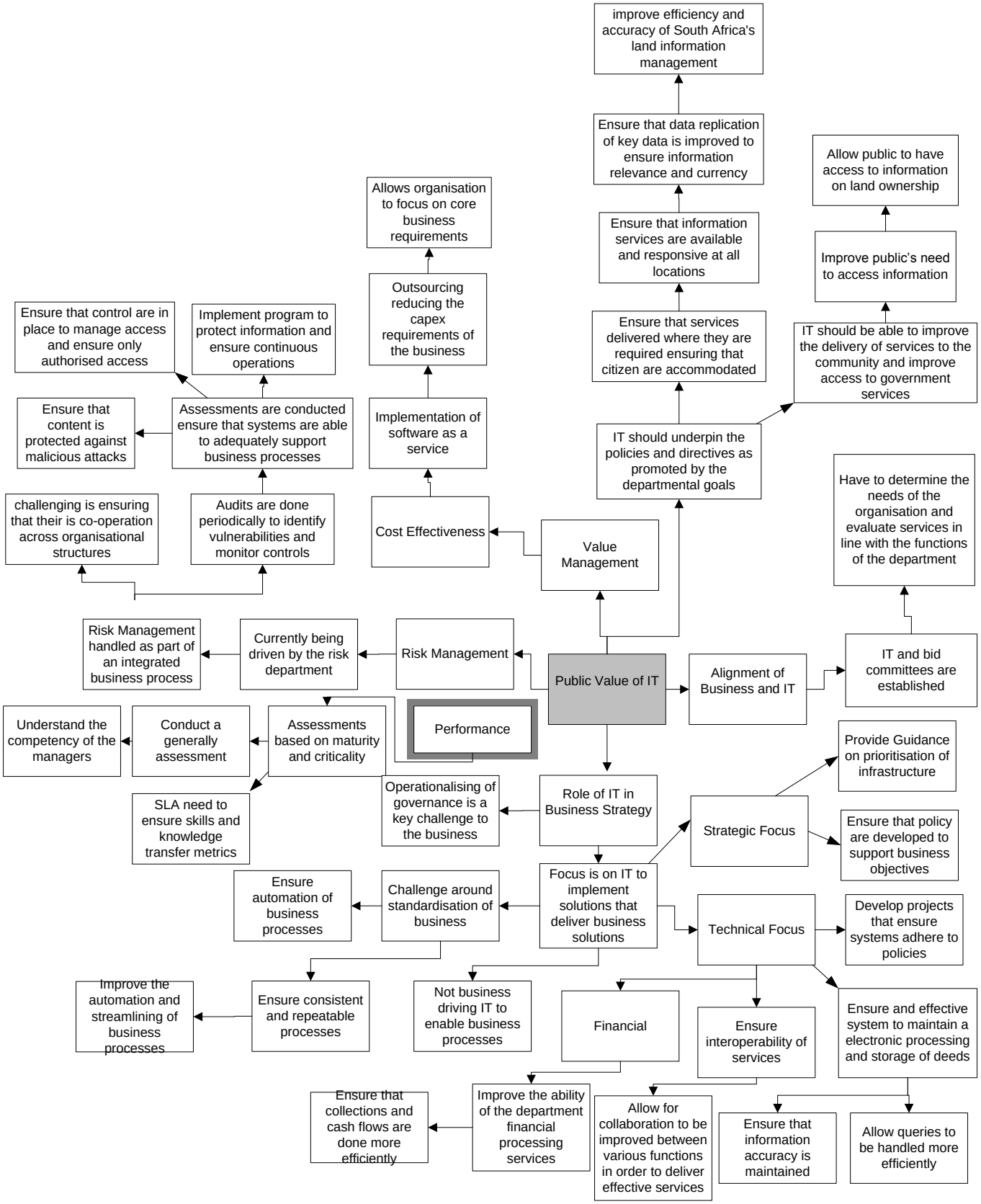


Figure 17: Cognitive Map for Interview 13

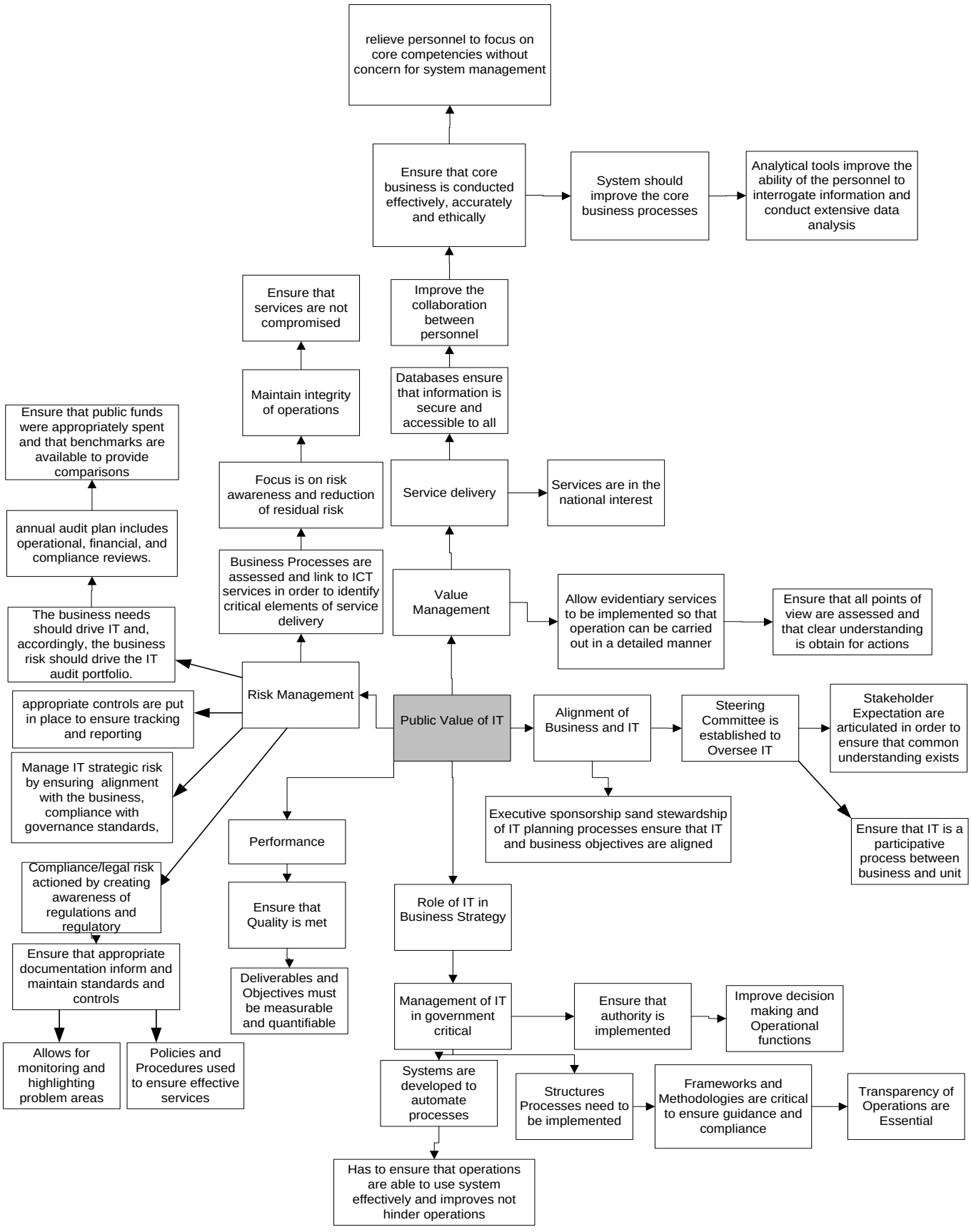


Figure 18: Cognitive Map for Interview 14

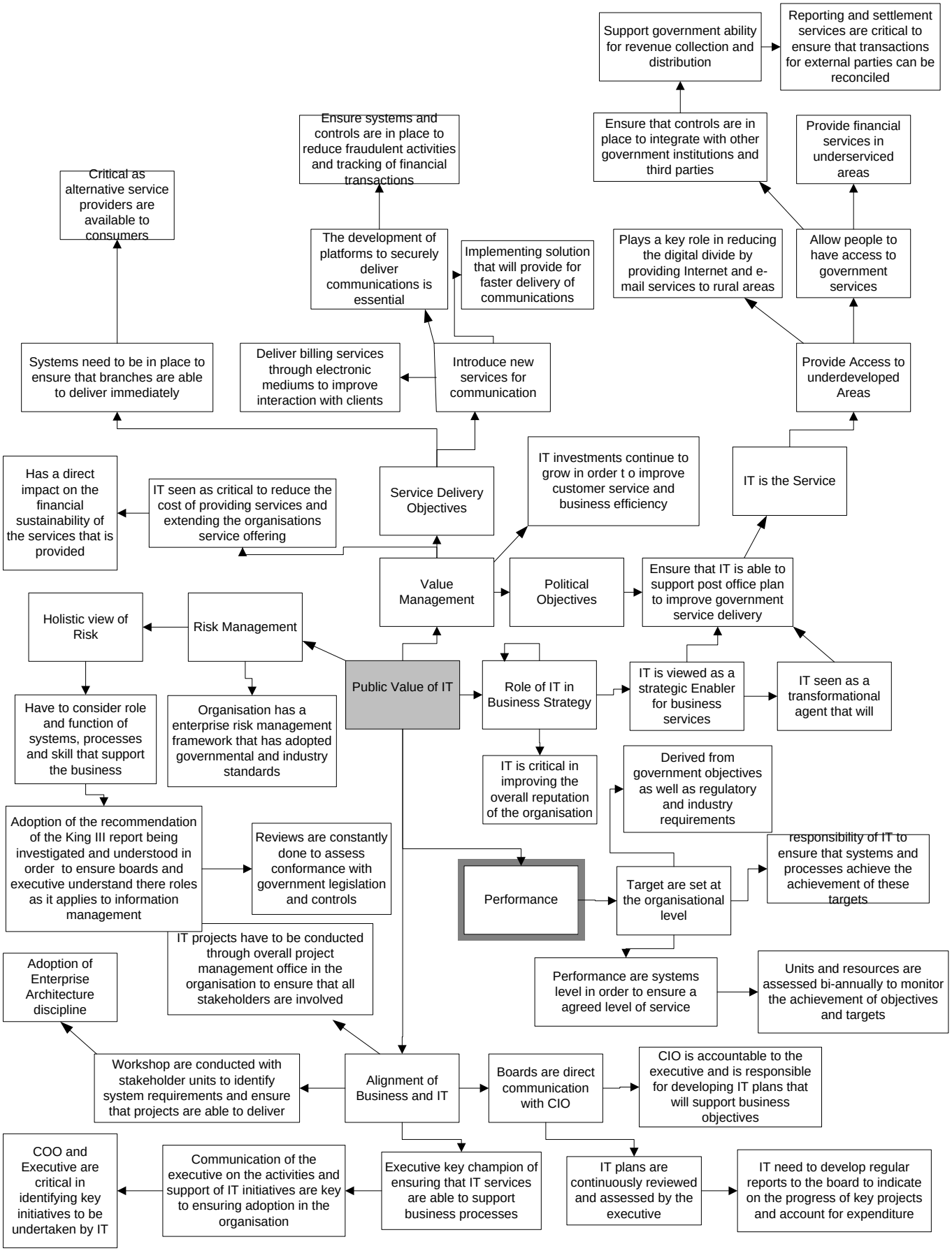
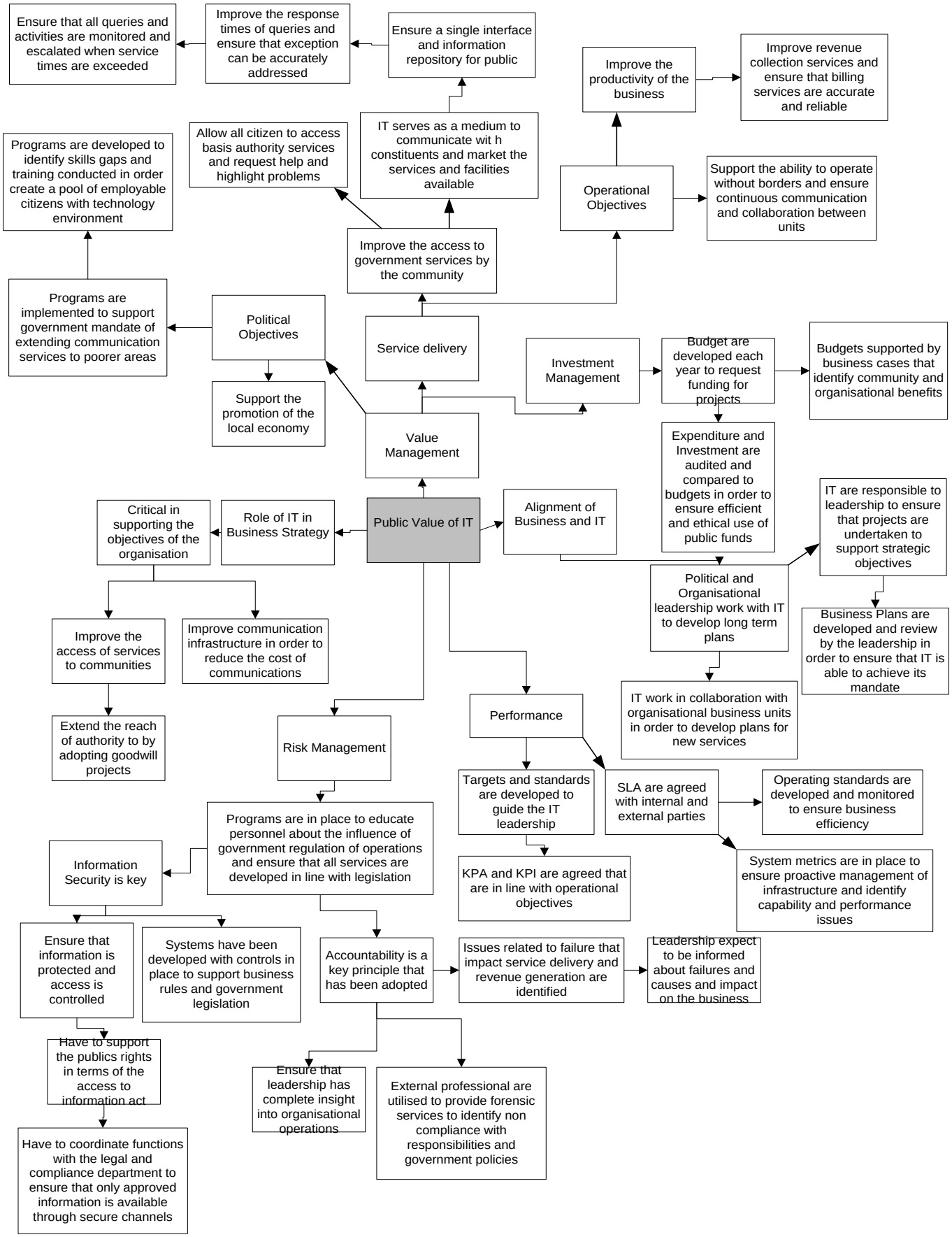


Figure 19: Cognitive Map for Interview 15



4.2. Research Finding

In total data was collected from 15 organisations within the public sector. All the respondents were intimately involved in the planning and management of the IT architecture and processes within their respective organisations. The organisations that participated in the process represented different spheres of government at national provincial and local level. In terms of the government clusters which were involved the responded included participants from the Social Sector Cluster, the Economic, Investment and Employment Cluster and the Governance and Administration Cluster.

The findings below provide and overview related to the role that IT plays within each of the responding organisations and the key processes related to IT Value and governance in the organisations. Each organisation's process maturity based on the governance domains has also been assessed. The framework used for this assessment was based on the COBIT Model (ITGI, 2007) and the definitions are documented in appendix D. The reason for assessing the organisational process maturity was done to understand the current state of the organisation's processes and how the organisations compared to each other. The COBIT model adopted does not intend to precisely measure or try to certify that a level has exactly been met (ITGI, 2007)

4.3. Organisational Findings and Process Maturity Evaluation

Organisation 1

This organisation plays a key role in the planning and assessment of the state of the economy. The IT entity within the organisation operated as an independent unit but was well aware of the overall strategy of the organisation, as the respondent was part of the senior executive structure within the organisation. The respondent was well informed about the role and impact of IT on the business processes in the organisation.

In terms of the business understanding of the role that IT can play in the organisation it was found that an IT steering committee had been put in place to assess the benefits and capabilities of IT within this organisation. The steering committee is representative of the entire organisation and in this way the business can influence the technology direction of the organisation. The respondent believes that this structure is a benefit to the operation of IT in the organisation as it allows both the technologists and management to develop a single view of the responsibility of IT in the organisation.

The researcher also found that the respondent was very well informed in terms of governance and controls that were required in order to deliver an effective IT service to the organisation. The processes in place within this organisation were very well developed as the need to ensure accuracy and credibility of the information services was paramount to the reputation of the organisation. In terms of the value of IT to this organisation the respondent felt that through the use of there services government has been able to benefit by developing more comprehensive infrastructure and social support plans.

Table 1: Organisation 1 Maturity Matrix

Maturity Matrix		
Domain	**Status**	**Evidence**
IT Governance	**Managed and Measurable**	The organisation has established processes for interaction with the business. All business unit managers are aware of governance practices in the organisation and there are predefined processes governing the operations of IT within the organisation. The IT department has established internal and external SLAs that provide guidance on the roles and functions of the IT organisation as well as their vendors.
IT Strategic Alignment	**Managed and Measurable**	IT consistently engages with the leadership of the organisation in order to understand the expectation of the business from IT in achieving the business objectives. The organisation has a documented IT plan which is revised on a regular basis in order to ensure that the business objectives are considered.
IT Value Delivery	**Managed and Measurable**	The organisation is well aware of the role that IT plays in achieving the objectives of the organisation. The value derived from IT investments are measured based on traditional investment measures and projects are approved based on their ability to benefit the business processes.
IT Risk Management	**Managed and Measurable**	There is good understanding of the risks to the business processes and the impact of an IT failure on the overall function in the business. IT is also part of a cross functional team that is responsible for identifying business, legal and operational risks. IT is then responsible for preparing plans to mitigate against technical risks.
IT Performance Management	**Repeatable**	The organisation has established a basic business and technical performance system. The overall performance of IT is assessed within the overall performance of the business. The systems and processes of IT are also assessed based on predefined metrics although no predefined targets have as yet been established.

Organisation 2

The organisation operates as a vehicle through which government investments are managed and was accountable to the national treasury. The IT entity in this organisation was under the leadership of the CIO who was the respondent to the research. However the CIO was not part of the executive management structure in the organisation and was accountable to the Chief Operating Officer (COO) and was therefore dependent of direction from the operational arm of the business to understand the strategic objective of the organisation.

In order to ensure that there was an alignment between the requirements of the business and the project undertaken by IT, a well develop operational framework had been put in place to address the technology requirement of the business. This operational structure included an architecture department that would map the business requirements into solution proposals. The approved solution was then given to the project management department in order to ensure successful implementation into the business.

The IT strategy within this organisation was driven by a steering committee which was headed by a senior executive and had representatives of both the executive and IT. However oversight for the investment and performance of IT was separated into different committees and as such it was the responsibility of the CIO to ensure that IT was able to achieve the objectives determined by the steering committee. In order to ensure that the CIO was able to manage this effectively a review and reporting process had been implemented in this organisation.

The value of IT to this organisation was considerable as information accuracy and currency was important for decisions to be made that would positively influence investments. It was therefore critical to this organisation that the management and control of IT ensured an effective service to the organisation.

Table 2: Organisation 2 Maturity Matrix

Maturity Matrix		
Domain	**Status**	**Evidence**
IT Governance	**Managed and Measurable**	The executive management team are involved in providing direction to the IT department in terms of their overall objectives. The organisation has an established scorecard through which deliverables and objectives are monitored. There are well defined units where functions are clearly outlined and there is an awareness of individual responsibilities.
IT Strategic Alignment	**Managed and Measurable**	The organisation has a well established organisational structure within which IT operates. The establishment of committees to oversee the operations and strategy of IT has resulted in a well coordinated approach to the achievement of IT objectives for the organisation. IT planning is conducted both for the IT function as well as for individual projects.
IT Value Delivery	**Managed and Measurable**	The organisation has to develop business cases for all IT investments which take into account both the costs and benefits to the organisation. Benefits are categorised on their ability to improve the overall business processes in the organisation.
IT Risk Management	**Managed and Measurable**	The organisation has an enterprise risk management framework in place. IT is required to participate in the processes of these teams and is required to ensure that systems and project risks are identified, prioritised and mitigated. IT also collaborates with the internal audit department to ensure compliance with legislation that could impact on achieving government mandate.
IT Performance Management	**Repeatable**	Objectives have been defined for IT and are documented within a balanced scorecard. The performance of the systems as well as the support staff are reviewed within a formal framework. The systems utilisation, availability and processing capabilities are all assessed.

Organisation 3

The organisation is involved in improving the access to government support for citizens. The role of IT in this organisation ensured that government was able to extend the delivery of services to remote areas in the country in a short period of time. However as this organisation had only been established in 2006, the IT structure was not that well developed. The primary function of the IT entity in this organisation was to ensure that the internal operations were able to implement processes within a short period of time and to secure, validate and maintain the integrity of information. Even though this organisation had a CIO governance controls, processes and policies were immature as the main focus was the implementation of systems to support the organisations mandate.

Table 3: Organisation 3 Maturity Matrix

Maturity Matrix		
Domain	**Status**	**Evidence**
IT Governance	**Repeatable**	The organisation has identified the need for a governance approach, and a senior manager has been selected to drive this process forward. However the executive has not yet fully recognised the importance of this function
IT Strategic Alignment	**Ad Hoc**	The organisation does not have a predefined strategic plan. Objectives have been agreed between the CIO and the rest of the business and these are articulated into project plans which the organisation is aware of.
IT Value Delivery	**Ad Hoc**	Most IT investments in this organisation are justified based on the project requirements. Those IT investments that are required for internal services need to show how they will improve the operation of the organisation. IT projects related to external services need to show how they will improve the ability of the organisation to execute its mandate. However currently no formal review or post mortem process exists to assess the impact of these initiatives
IT Risk Management	**Ad Hoc**	The identification and management of IT risks are the responsibility of the CIO who will communicate with the CFO in order to understand the technical risks and their impact on the business. No overall risk management framework exists within the organisation and each individual department is required to develop independent plans.
IT Performance Management	**Ad Hoc**	No formal performance management processes currently exist within this organisation. All services and processes are managed reactively and IT is expected to respond to performance problems in this environment. There are no formal checkpoints established to review the performance of IT in the organisation.

Organisation 4

Historically there had been no strategic focus on the role of IT within the organisation. It had previously only been seen as supporting the business processes. However due to the recent changes within the executive structure in this organisation IT has now become a critical element to the organisational turnaround strategy. A new CIO had been appointed who represents IT at the executive level and is accountable to the CEO. The new objective for IT in this organisation is to enable the business to become a sustainable enterprise.

Due to the recent appointment of a new management team within this organisation the understanding of the IT practice in this organisation is fairly limited at the current stage. However the CEO does understand that in order to turn the organisation around, IT would need to reinvent itself from a support function into a core business service which would drive the business processes. The business believes that in order for the public to regain confidence with the institution, IT will need to ensure that the credibility of the services is rediscovered by improving accountability and preventing the manipulation of information.

In order to ensure that IT is able to deliver on its new mandate, a relationship has been encouraged between the business' risk, audit and compliance practice and IT. This new relationship is being driven from within IT by a governance unit who are responsible for ensuring that there is an understanding of the objectives of the organisation as well as the business policies and that these are built into the systems and processes of the IT entity. There has also been focus placed on the role of audits and compliance for IT. And both IT and business, in the form of internal audit are involved in assessing the capabilities and controls of the organisation.

Previously IT in the organisation was held back due to the bureaucratic processes that had been put in place and therefore IT value was not actively managed. However the new management team has ensured that specific targets are derived for IT based on the objectives of the organisation. In addition the investment in IT and the ability of IT to add value to the business are monitored through formalised planning and review processes where the roles and function of IT to specific business processes are assessed and evaluated.

Table 4: Organisation 4 Maturity Matrix

Maturity Matrix		
Domain	**Status**	**Evidence**
IT Governance	**Ad Hoc**	The new management team has identified the need for an overhaul of the governance practices within the organisation. A new unit has been established within IT to oversee the implementation and compliance with governance practices
IT Strategic Alignment	**Ad Hoc**	Due to the recent appointment of a CIO in this organisation a new emphasis has been place on aligning the IT and business objectives. Very few formal processes existed previously, however the role of IT going forward is seen as key to the organisational turnaround.
IT Value Delivery	**Non Existent**	IT has always been seen as a cost centre and needs to support the business processes, no continuous management of IT over the lifecycle is being done, although the organisation are reviewing the manner in which IT value is being measured.
IT Risk Management	**Defined**	IT risk management is driven from within the overall risk management department. This unit engages with IT to ensure that all systems and processes are assessed and the risk of failure or unavailability is understood. Those plans that account for critical risks are driven by enterprise risk management who need to provide funding for these initiatives.
IT Performance Management	**Defined**	The IT performance management processes in the organisation have recently been reviewed and updated. The previous performance management framework was subject to manipulation and management used this system to prevent personnel from achieving targets as no metrics existed that could be independently verified. Specific targets have been set and performance measured in terms of attainment

Organisation 5

The organisation has a critical role in achieving government's objective of improving infrastructure development in rural and poor communities. The organisation is accountable to the department of public works in terms of its mandate and is involved in various initiatives that extend government services to historically deprived communities.

IT within this organisation does not function as an independent entity as it is accountable to the CFO. In order to overcome the challenge of not being represented at executive level, the senior management team in IT are allowed to participate in the organisational planning sessions. During these sessions there are specific objectives derived for IT in order to support the ability of the business to deliver on its mandate. These goals and objectives are documented and it is the responsibility of IT management to account to the CFO and ultimately to the CEO of the achievement of the objectives during executive meetings.

Additionally there is a steering committee that has been established in this organisation whose role it is to understand the projects and investments related to IT and who are responsible for understanding the impact of IT on business processes. This committee is represented by various senior managers in the organisation who focus on assessing the role of IT to facilitate organisational effectiveness within their own area of responsibility.

The value derived from IT in the organisation currently is managed in the form of formalised reporting and review sessions that are held with the board. During these sessions IT management are tasked with presenting a full quarterly overview of the current state of IT as well as the intended projects that IT will undertake. The challenge that exists for IT is that these sessions are focussed on cost and financial implications and therefore IT cannot provide a full assessment of the benefits that are derived from IT to the organisation.

Table 5: Organisation 5 Maturity Matrix

Maturity Matrix		
Domain	**Status**	**Evidence**
IT Governance	**Ad Hoc**	No formal governance framework has been adopted within this organisation. The measurement and outcomes for IT are done at an operational and project level, and it is the duty of the executive head of IT to ensure compliance with the organisational objectives.
IT Strategic Alignment	**Defined**	The IT department is required to submit formal plans on an annual basis to the executives which indicate the objectives of IT and how they will support the business. However these plans are not iterative and are purely based on projects and service functionality.
IT Value Delivery	**AD Hoc**	All projects are subject to a post mortem and IT need to account for the expenditure within the IT environment. IT are also required to get involved the annual budget preparation and need to constantly provide the business with feedback based on the requested funding.
IT Risk Management	**Defined**	A Separate risk management department exists within the organisation. It is the duty of the IT department to provide this unit with a plan identifying the potential risk and threats to the environment.
IT Performance Management	**Ad Hoc**	Currently IT believes that the systems and processes are not managed well as there are no agreed targets that need to be met by IT. The only two measures that are currently being actively monitored are systems availability and project costs.

Organisation 6

This organisation operates independently of government control but is accountable to the finance ministry. The organisation plays a key role improving the economy by investing in projects that will support the government's industrial expansion program. Within this organisation, IT functions as a separate business unit who has an executive head but has no representation at board level and is accountable to the CFO. The organisation has identified this as a short coming of the business structure and believes that a CIO would add value to the overall function of IT within the organisation as it would allow the unit to lobby the executive directly for IT initiatives.

In order to ensure that IT are able to support the objectives of the business the executive head of IT is allowed to attend the business planning sessions as an observer but is not directly involved in the planning process. Separate planning sessions and reviews are also conducted with IT Management on a bi-annual basis in order to understand the projects to be undertaken and changes required to the systems to support business processes. In addition a steering committee has been established which is chaired by the CFO. It is the duty of IT to report to this committee on project performance as well as operational activities within the department.

Apart from the financial reviews which are conducted to assess the investment and compare the project costs against business cases very few measures are place to assess the value of IT to the business, Even though IT has played a key role in improving the efficiency of the processes and reduces the bureaucracy that existed in terms of allowing funding to be directed to projects. IT has also been key in improving and assessing the progress of the organisation's investments and allowing the organisation to get an updated view of all project performances. However there has not been any direct measures that have been put in place to assess the role of IT within these areas.

In terms of risk management, IT is also very well aligned with the overall risk program of the organisation. The overall framework within the organisation encompasses the IT entity, and IT is involved in the overall development of the risk framework within the organisation. In order to mitigate against these risks and to ensure compliance with organisational policies the IT department is subject to audits. In the first instance the internal audit reviews the processes and controls that have been implemented in the department as well as those integrated into the systems of the organisation. Secondly the IT operations within the organisation are subject to an external assessment where best practices are evaluated as well as a review of the systems and controls adherence to legislation and government requirements.

Table 6: Organisation 6 Maturity Matrix

Maturity Matrix		
Domain	**Status**	**Evidence**
IT Governance	**Optimised**	The organisation is fully aware of the industry practices and has adopted a practice which has ensured that IT processes and services are managed. Problems within processes are identified and actions are generated to ensure that these issues are resolved.
IT Strategic Alignment	**Managed and Measurable**	The IT executive is responsible for establishing plans for the organisation based on the overall outcomes of the strategic planning process in the organisation. These plans are part of the overall business plan and are subject to review of the board on a regular basis.
IT Value Delivery	**Managed and Measurable**	IT investments are assessed based on the ability to provide value to the processes that they are supporting, as well as on how effectively projects are able to be met within the required budget. Overall IT investments are reviewed on how effective they have been in ensuring that the businesses can respond to client requirements. Internally the value derived from IT is also assessed by the organisational users.
IT Risk Management	**Managed and Measurable**	A comprehensive risk framework has been put in place. IT works with the risk department to identify, prioritise and manage the risks in their environment. The organisation also continuously utilises the services of external experts to assess the technical risk environment and measure the potential impact of an incident to the business. Risk plans are subject to business review and are continuously updated to take into account current trends in the environment.
IT Performance Management	**Repeatable**	The organisation has acquired tools and systems that are used to monitor the overall performance of the systems. System reliability and availability are continuously monitored and the response times of systems are tested to ensure optimum performance. The services are also continuously monitored and all service requests are tracked and measured against predefined standards.

Organisation 7

The organisation was accountable the MEC of Finance for the Gauteng provincial government and are mandated with providing centralised financial and supply chain management services to the province. Furthermore this organisation is responsible for ensuring that the public are able to access government services within their communities.

The organisation's senior IT official is the CIO who is a member of the executive board and is therefore fully aware of all strategic decisions that are made in the organisation. In this manner IT are able to have a direct insight into the role and function that they are required to play in the organisation. Furthermore IT has the additional function as a medium through which communities and citizens are able to access government information.

There are various formal structures in place within this organisation to which IT are accountable. The most senior board is currently the IT steering committee who are an advisory and review structure and who are tasked with assessing the financial and operational impact of IT in the organisation. This committee are also responsible for reviewing the human impact that any IT change may have to the operations of the organisation, as there is a strong focus in ensuring participative change management while retaining and retraining the personnel in the organisation.

Secondly the organisation has to present all business proposals and solutions to the departmental acquisition council who are tasked with reviewing the business and financial impact of IT and assessing the solution in line with government directives.

The third structure in place are the project committees who need to ensure that all government programs are supported by the department's IT services and that the systems are configured to ensure that the organisation is able to deliver on its mandate. The CIO is actively involved in all project committees in order to ensure that the key objectives of the business are maintained and in order to ensure that that bottlenecks originating from outside of IT are noted and raised with the executive of the organisation in order to ensure that service delivery is not jeopardised.

Table 7: Organisation 7 Maturity Matrix

Maturity Matrix		
Domain	**Status**	**Evidence**
IT Governance	**Optimised**	The organisational executives have identified the management and control of IT as critical to achieving the overall strategic objectives of the organisation. External professionals have been recruited to assist the established IT Governance practice to refine the processes related to IT Governance in the organisation.
IT Strategic Alignment	**Managed and Measurable**	The IT plan in the organisation is based on forward looking planning and takes into account the current needs of the organisation as well as the key role that it can play in allowing the government as a whole to achieve their objectives.
IT Value Delivery	**Managed and Measurable**	Due to the stringent requirements to account to the provincial legislature on all investments. IT is also required to provide the business with an overall report on the performance of the investments and how they had been able to improve the business process. IT project progress reporting is also seen as essential for this organisation so that they can assess the value of IT to the overall ability of the organisation to engage with the public.
IT Risk Management	**Managed and Measurable**	The internal audit department is responsible for ensuring that the business risks of IT are identified and documented. IT is responsible for developing plans to mitigate against these risks and drive projects to implement responses to these risks.
IT Performance Management	**Repeatable**	The organisation has established performance agreements with the business units in the organisation. These agreements are articulated in the form of service availability and are then decomposed into the various element measures that all work together to provide the service. The tools have been put in place to monitor all systems and reports are provided to the business users.

Organisation 8

The organisation is accountable to parliament and is responsible for ensuring that the protection afforded to citizens within the framework of the constitution is upheld. The IT entity within the organisation is under the control of a deputy director who in turn reports into the head of finance for the organisation. All IT initiatives within the organisation are driven by the IT head who needs to justify the investment as the entity is viewed as a cost centre. The role of the CEO of the organisation is critical in order to ensure that IT projects are undertaken and that IT is able to provide the necessary support to the functions of the other business units.

In order to justify the value that is produced by IT, the organisation has adopted a traditional financial management methodology. The deputy director is responsible for developing the budgets that are required by the IT department. These budgets are then reviewed by the senior management team in the organisation and assessed in terms of the benefits that can be derived from the other business units in order to improve the efficiency of the services provided by the organisation. The key drivers for this organisation are the extension of services to areas where transportation and access to physical locations are a challenge.

In terms of the risk management methodology adopted by this organisation, all risks are assessed in terms of the impact that they would have in preventing the organisation from achieving its government mandate. Internally processes and systems are assessed by the auditor-general in order to understand if there is compliance with government legislation and whether any abuse of there mandate has occurred. IT is subject to the same process as other business units as IT has to ensure that there are adequate controls in place to ensure that no process or policy of the organisation is circumvented.

Table 8: Organisation 8 Maturity Matrix

Maturity Matrix		
Domain	**Status**	**Evidence**
IT Governance	**Non Existent**	The organisation views IT as a support services and the management is purely based on cost and budget controls.
IT Strategic Alignment	**Ad Hoc**	IT is not directly involved in the overall planning in the organisation and is depended on divisional planning in order to understand their objectives. The IT management are also responsible for developing business cases in order to justify all funding requirements.
IT Value Delivery	**Non Existent**	IT has to account for all their expenditure to the finance department. All funding is subject to a business justification process. However no overall assessment of the benefits that are derived from IT is conducted.
IT Risk Management	**Ad Hoc**	No formal risk management framework exists within the environment. IT is totally responsible for ensuring that services are continuously available to the business. The IT department has developed strong contract and SLAs with external vendors in order to ensure that business continuity is not affected.
IT Performance Management	**Non Existent**	No system measures are currently in place to measure service internally. However all services that had been outsourced by the organisation are subject to regular reviews and are measured against predefined performance criteria.

Organisation 9

The organisation exists under the control of the department of environmental affairs and tourism, and plays a key role in the planning of key government services related to environmental conditions. Historically the role of IT within this organisation was seen as supporting the business processes. However due to the closer interaction with international peers as well as a closer integration with other government services and departments within the public enterprises department, the role of IT has evolved as a strategic pillar on which the business is built. Furthermore the cooperation with government departments at provincial and municipal level in terms of disaster management planning and rescue has resulted in the integration of IT becoming critical.

Currently the head of IT has the delegation of a senior manager who is accountable to the COO and their goals are derived from the overall operations mandate. Due to the fact that there is no direct representation of IT at the executive level, there is a strong dependency on IT to ensure that they are able to deliver there message effectively within the operations environment. IT however does have the benefit of being involved in the overall strategic planning process of the organisation, and are therefore able to understand what is required of them to deliver an effective service to the organisation.

The organisation is also very up to date in terms of the current practices related to governance and controls within IT. This organisation is the only one of those that had participated in this study that are actively looking at implementing the recommendations of King III into there governance charter. The process of ensuring IT Governance in line with the recommendation of King III is being driven from the director general's office, and will play a key role in the director general's assessment of the IT function in the organisation.

The management and reporting of the value derived from IT in the organisation is based on historical business plans that are reviewed annually in terms of the unit's ability to execute and support the business within the financial and cost metrics committed to the division. However the IT unit are not limited to these reviews only and are allowed to make representation to the board if they believe that a project which requires a substantial investment will add value to the business.

There is also a good understanding of the risk within the IT environment and the impact that they have on the organisation. The risk management process in the organisation is driven by the board secretary who is tasked with liaising with each business unit to map the potential risks against the key activities of the business. IT is then involved with the business to categorise and prioritise the risks and then prepare plans to support continuous operation of key processes in the organisation.

Table 9: Organisation 9 Maturity Matrix

Maturity Matrix		
Domain	**Status**	**Evidence**
IT Governance	**Managed and Measurable**	The executive team has involved IT in the overall planning function in the organisation, including the corporate governance planning. This organisation is in the process of adopting the recommendation of the King III report and is looking at its implications for the public sector. All IT processes in the organisation are assessed and benchmarked by an external party
IT Strategic Alignment	**Managed and Measurable**	The IT unit are involved in the overall business planning process, and also need to provide reports to the business on the progress made in the IT department over a predefined period. IT also provides the business with a report on both the long term and short term initiatives that will be undertaken by unit in order to support the business. IT also prepare annual plans for the unit which are reviewed by the business to ensure alignment with the overall objectives in the business
IT Value Delivery	**Ad Hoc**	The organisation does provide continuous feedback to the business on large scale projects. All project funding needs to be justified to the board, and expenditure is monitored in terms of whether there are any exceptions to pre approved plans. Due to the commercialisation of various services the organisation is beginning to look at reviewing the total benefits that are obtain from an investment
IT Risk Management	**Managed and Measurable**	The risk management process in the organisation is driven by the board secretary who is responsible for preparing the overall risk management plan. Furthermore Disaster Planning and Business continuity are driven from the CEO's office. The CEO has site of all IT risks which are all reviewed by the board as part of the responsibilities as outlined by the King III report.
IT Performance Management	**Repeatable**	IT has monitoring tools that measure individual systems, but there is no service management system currently in place. The organisation also proactively monitors the performance of individuals within IT and outcomes are used to develop training and intervention programs that will improve the service to the business.

Organisation 10

This organisation operates under the auspices of the department of local government and is responsible for ensuring that there is co-ordination and compliance across municipal structures in the country. The IT unit is represented at executive level by a director and who reports to the chief financial officer and do not have a direct influence on the role and function of IT in the organisation. The main function of IT in the organisation is to ensure that all members are able to gain access to information. The unit is also responsible for ensuring that members of the association have the required infrastructure to take advantage of the available information services. Furthermore the unit is actively involved in communicating and training the executive management on how they can utilise the IT services to improve their own productivity within the organisation.

In order to ensure alignment between the business and IT functions within the organisation, the IT director is required to provide detailed plans to the business on the functionality and capabilities of IT. In additional regular audits are conducted by external consultants and the findings are presented to the business in terms of the current state of IT and the programs that need to be put in place where shortcomings are identified with the current IT environment. The organisation does not have any formal structures to provide guidance to IT.

In order to measure the value that is provide by IT to the organisation, specific performance metrics have been put in place to measure the availability and reliability of IT to support the business. IT has to work within a strict financial environment but there are no real investment measurements that are used to measure IT value and the organisation does not feel that these are warranted at this stage as the budgets are developed from available funding of members and not directly from government revenues.

The main criteria for assessing the risk that IT poses to the organisations is based on the impact that IT may have to preventing members from accessing services that could then impact there ability to deliver services to there constituents. The organisation ais also bound to specific controls and policies that are derived from the public finance and municipal finance legislation, the systems that are put in place by the organisation are therefore audited regularly to ensure that the organisation is not exposed to any manipulative practices that could impact the viability of the organisation.

Table 10: Organisation 10 Maturity Matrix

Maturity Matrix		
Domain	**Status**	**Evidence**
IT Governance	**Non Existent**	The organisation manages the IT department based purely on deliverables and there are no formal processes through which IT can engage with the business leadership as a whole.
IT Strategic Alignment	**Ad Hoc**	There is no formal reporting process for IT plans. However IT does need to keep the business informed about their initiatives. It is also the responsibility of IT to drive the communication between the business and the unit
IT Value Delivery	**Non Existent**	Due to the limited financial resources that are available to the organisation, all IT expenditure is assessed based on the total cost of the solution. IT is continuously looked on to provide cost cutting measured and utilise systems that will reduce the operational costs of the business.
IT Risk Management	**Repeatable**	The organisation has a risk committee who are responsible for developing the organisational risk plan. IT risks are reviewed in terms of the impact on their business, and are measured in terms of their financial and operational impact. Business assists in identifying threats and developing contingency plans.
IT Performance Management	**Non Existent**	Apart from ensuring that services are available no tools are in place to monitor system performance. The performance of the IT personnel in the organisation is only assessed in terms of being available to resolve user problems.

Organisation 11

This organisation's core focus is to ensure the stability of the economy and development of financial and statistical information that would assist the government in developing plans that would maintain the health of the economy. IT within this organisation is part of the Business Systems and Technology Department who are responsible for ensuring that services and processes are adopted in order to empower business. The technology department is under the control of a senior manager who reports to the management board.

The group has a well developed IT strategic framework which provides an overview of the primary roles, functions and services that need to be provided to the organisation. The technology unit has also been successful in determining the critical success factors and success measurement criteria for the services which they offer. This unit has developed an effective communications plan in order to ensure that there is an awareness in the organisation of the strategy and services of the group.

The management of the alignment between the role of IT in the organisation and the expectations of the business is actively pursued by the technology group. Within the technology and services groups senior managers have been identified who are all responsible for managing the requirements and expectations of the different business units within the organisation. Specific operational contracts are developed for each unit and are reviewed on a regular basis in order to ensure that the services are effectively supporting the business.

The organisation also has a well define committee structure that are responsible for reviewing the projects and initiatives that will be undertaken by the business. IT projects and services are also subject to a formal review and assessment where investments and expenditure are examined to determine the success and viability of IT.

Table 11: Organisation 11 Maturity Matrix

Maturity Matrix		
Domain	**Status**	**Evidence**
IT Governance	**Managed and Measurable**	The organisation has a well established control and monitoring environment. The unit also has a specific manager that has been appointed for the development of the IT Governance framework. The organisation has a well documented guideline that ensures that all senior managers are aware of the policies and deliverables of the group.
IT Strategic Alignment	**Managed and Measurable**	The senior management of the technology are well informed about the mandate and overall duties of the organisation. The Executive management team are also regularly updated on the functions and duties of IT in order to ensure that there is co-ordination between the business and IT.
IT Value Delivery	**Managed and Measurable**	The organisation has a strong emphasis on developing strong business justifications for any of the project that they are involved with. The organisation also believes in assessing the intangible benefits that can be derived from any IT initiatives as these could relate to process improvements that may not be considered through traditional financial calculations.
IT Risk Management	**Managed and Measurable**	Due to the highly confidential nature of the operations within the bank, the technology group has a well developed risk management process in place. The risks are identified from both a business and technical perspective and all risks need to be reported to the risk committee. This committee need to ensure that those risks that would jeopardise the operations of the organisation need to be proactively managed and contained.
IT Performance Management	**Managed and Measurable**	The organisation has a well established systems and process performance management framework in place. This framework takes into account the both the overall performance of the IT function in delivering an efficient and effective service to the business. The group also has regular feedback with user departments to determine the perception of the services being delivered.

Organisation 12

This department plays a key role in ensuring that the government is able to redress the distribution of land ownership that existed in the past. The organisation also plays a critical role in the development of spatial planning and maintaining an accurate account of the ownership of land within the country. Due to the diverse nature of the operations undertaken by this department, IT plays a significant role in ensuring that business solutions are delivered that supports the objectives of the department. Furthermore the IT systems and processes that have been adopted by this organisation needs to ensure that there is access to the services provided by the department nationwide and that there is no one that is adversely affected by the unavailability of systems.

The IT group in this department is currently run by the CIO who is accountable to the senior leadership in the organisation. The CIO is directly involved in the departmental strategy planning processes and is responsible for ensuring that IT have a clear plan to support the function of the department. The organisation also has an establish IT review panel and tender evaluation process that ensure that the business and well as technology objectives are addressed in any solution or project that IT are involved in. The department also utilises the services of the State Information Technology Agency (SITA) in order to ensure that they are able to benefit from the governments centralised procurement and negotiating power, as well as to maintain the operating standards and system specifications in order to achieve better collaboration across the public sector.

The challenge that IT currently has though is that the leadership need to understand the full impact of the various legislative and regulatory frameworks on the IT services in the organisation. IT currently has the problem in that the roles and functions as indicated through various legislative measures have not adequately been interpreted into specific responsibilities for senior management in the organisation. IT is therefore solely responsible for developing policies that ensure that there are processes and systems that are compliant with the required standards.

Table 12: Organisation 12 Maturity Matrix

Maturity Matrix		
Domain	**Status**	**Evidence**
IT Governance	**Defined**	The need for IT Governance is understood by the business, specifically as they have to ensure compliance with multiple acts and industry standards. The department currently utilises the services of a professional services organisation that are tasked with ensuring that there is a successful deployment of IT Governance structures and processes in the organisation.
IT Strategic Alignment	**Defined**	The department is intimately involved in understanding the objectives and goals of the organisation as they are determined by the political mandate. The planning of IT is done in collaboration with the overall planning of the department and the reporting on IT performance and investment is considered essential in terms of the department's feedback to their political principals.
IT Value Delivery	**Defined**	There is a strong emphasis within the department on the need to justify the expenditure on IT, especially due the constraints on the overall departmental budget in order to perform there core functions. The justification of IT investment within the organisation is focussed on ensuring that projects are cost effective and are able to leverage the economies of scale that the government has with the technology supplier industry. The department also looks at the social implications of there expenditure and investment in order to determine whether IT has improve the ability of the public to engage with government and access departmental services and information.
IT Risk Management	**Defined**	The responsibility for risk management in the department currently resided with a specific unit, who need to engage with the various operational units within the department in order to perform a total assessment of the business processes and the related risks that exist. IT together with the risk department then develops and plans to ensure service availability.
IT Performance Management	**Defined**	The department is currently in the process of developing a performance management system that not only looks at the technical standards and metrics of the IT systems but can assess the maturity of the processes in the organisation and understand the competency of the managers in order to identify where training or intervention is required to improve service delivery and support.

Organisation 13

This organisation plays a critical oversight role within government to ensure compliance with the legislation and policies that are adopted by the government. The organisation is also responsible for ensuring that public officials act responsibility and are accountable for there actions, this institution is responsible for ensuring that government employees act within the ambits of the law and need to account for there actions.

The role of IT in this organisation is critical in that it allows the employees of the organisation to operate from various environments and still be able to communicate and collaborate securely with colleagues and principals. The need to ensure information integrity and the accuracy of research and evaluation systems is also paramount to ensuring that the organisation is able to fulfil its mandate from government. Furthermore the storage and retrieval of information for tracking historical data of various government institutions is a critical objective for the IT unit.

The delegation of responsibility as far as IT is concerned is structured in order to ensure that the management of information and infrastructure are separated, as both are seen as critical to the overall success of the organisation. The structure adopted by this organisation also ensures that the organisation can fully leverage all technology and information at there disposal by ensuring specific oversight for critical systems and processes.

Furthermore the involvement of the business in the assessment and planning of IT projects are well established in the organisation. All IT initiatives are driven through a committee process which is chaired by an independent executive. These committees are responsible for ensuring that there is a clear understanding of the project objectives as well as the implications for the specific business units. The project committees need to ensure that they clearly understand the value that can be derived from IT projects.

Table 13: Organisation 13 Maturity Matrix

Maturity Matrix		
Domain	**Status**	**Evidence**
IT Governance	**Managed and Measurable**	The organisation continues to develop and evolve the processes in order to be aligned with the industry standards and best practices. Personnel in the organisation are trained in the most recent trends and practices within the industry and are able to adapt these practices into there environment. The organisation is also an established contributor of various industry forums that are responsible for developing operating standards.
IT Strategic Alignment	**Managed and Measurable**	The IT entity in the unit is under the leadership and control of an executive head that is accountable to the chief operating officer for the delivery of IT to the organisation. The IT leadership within the organisation needs to report to an independent panel on the performance of IT in the organisation, and are mandated to ensure that IT projects are aligned with the overall business strategy.
IT Value Delivery	**Managed and Measurable**	All IT investments in the organisation need to be accounted for based on the ability to improve business processes and delivering an effective service to the government. The expenditure on IT within the organisation also needs to be accounted for based on predefined business cases and approved budgets.
IT Risk Management	**Optimised**	The organisation has a comprehensive risk management framework in place that considers both the technical as well as business impact of any system and process in the organisation. Risk management in this organisation is conducted to ensure that the unit complies with the required legislative and regulatory responsibilities and also to ensure that the services that are delivered by the organisation are not compromised. Systems, processes and control within the IT environment are subject to regular assessments in order to ensure the continued ability of IT to support the business processes
IT Performance Management	**Managed and Measurable**	The organisation has adopted a comprehensive review system that has defined performance indicators and success measures for all services and processes that are offered. The services offered by IT to the organisation as well as the overall performance of IT are constantly reviewed by the organisation to ensure that IT is able to deliver a valuable service to the business.

Organisation 14

This organisation plays a key role in providing communication and logistical services to the public, although the organisation is under the control of the government, unlike other institutions in this research the organisation does have a profit motive along with it obligation to provide information services in underprivileged areas in the country. The role of IT in this organisation is seen as critical to enabling business services and is an agent for the transformation of the organisation's services offerings.

The alignment of IT in this organisation is well established as the executive management team are seen as driving the technology agenda in the organisation in order to improve the automation of the business processes, especially in the environment where there is direct competition from corporate service providers. Furthermore due to the adoption of a new business model, IT was identified as a core business unit within the organisation where competencies and skills were needed in order to ensure that the organisation was able to leverage its investments to improve service delivery and achieve and advantage in the market.

There has also been a review of the manner in which IT projects are undertaken within the organisation. The focus of this exercise was to identify areas of common services across the various business units in the organisation so that a single strategy and roadmap could be adopted in these environments in order to reduce the operational costs within the organisation.

Table14: Organisation 14 Maturity Matrix

Maturity Matrix		
Domain	**Status**	**Evidence**
IT Governance	**Managed and Measurable**	The organisation has adopted various best practices and service management methodologies in order to assess the various processes within the IT environment, and to develop processes that had previously not existed. Due to the fact the organisation not only has a mandate from government but also has strict compliance and operating standards that they need to adhere to in terms of offering financial services, comprehensive policies and operating guidelines have been established to ensure all functions are monitored, controlled and subject to evaluation.
IT Strategic Alignment	**Managed and Measurable**	The executive leadership within the organisation understand the critical role that IT plays in the organisation, and have committed to ensuring that IT are involved in all strategic planning activities in the organisation. The organisation also has appointed a CIO who is part of the executive leadership team in the organisation. The CIO and the IT leadership is responsible for articulating the needs of the business into technology solutions. Furthermore the introduction of an enterprise architecture discipline has ensured that a business process is mapped to a specific IT service and solution. All IT projects conducted by the organisation are done under the awareness of the enterprise project management office to ensure there is co-ordination amongst the various business units in the organisation.
IT Value Delivery	**Managed and Measurable**	The investment that is made in IT within the organisation has to be accounted for to the political principals in order to justify and report back on the organisation meeting it political and social objectives. However due to the corporate nature of the business, IT also needs to ensure that all investments are considered based on the return and financial impact they will have on the business.
IT Risk Management	**Managed and Measurable**	The IT group are required to engage the enterprise risk management discipline in order to develop the IT risk management plan and process. IT risk within this organisation is not only looked at from a systems perspective but all considers the role of critical resources and skills that are required to maintain the IT environment. Furthermore due to the nature of the business being conducted by this organisation specific policies and controls are adopted to protect the transactional environment.
IT Performance Management	**Meanaged and Measurable**	The service provided by the IT organisation to the rest of the business are underpinned by operating contracts and IT has to adhere to specific system performance criteria that are determine by the business based on the business requirements and industry standards. The organisation has also adopted a

		performance review system that assesses the systems, processes and resources within the environment. The assessments assist the organisation in identifying areas that require improvement as well as to identity and retain talented individuals.

Organisation 15

This authority plays a vital role in ensuring that government services are delivered to the citizens. Its mandate is to ensure that the public has access to primary services including, protection, healthcare and utilities. Furthermore the authority has a vital role to play in providing information to the public. Throughout this organisation IT services are pervasive and the entire operation of the authority is conducted on automated processes that are driven by IT. The organisation is also ensuring that the digital gap that exists due to historical access to wealth is reduced by supporting the deployment on internet and communication services on its own infrastructure in public areas.

The planning and development of the IT strategy within this organisation is driven by the IT directorate who are accountable both to the political leadership in order to support the socio-economic objectives of the government, and the organisational management who are responsible for delivering services to the constituents. Due to the beneficial position that this authority and similar structures within the country find themselves in terms of ownership of infrastructure, IT is able to leverage this position to introduce new services to support the development of the local economy.

In order to ensure that the funds are appropriated to project where they can add value, IT are required to develop annual financial and business plans that outline the investment and expenditure that will be undertaken by the directorate. These plans are subject to organisational and council approval and are reviewed on a regular basis in order to ensure that funds are spent appropriately. The value of the expenditure in this authority is justified both on the ability to achieve the political objectives in terms of service delivery and organisational objectives which are required to drive efficiency and improve customer interaction with the authority.

The review and management of risk in the authority is comprehensive as they are subject to both internal and government audits. These audits ensure that controls and policies are in place to align the organisation with the specific legislation that governs there operations and to ensure that plans are in place to prevent the failure and availability of services.

Table 15: Organisation 15 Maturity Matrix

Maturity Matrix		
Domain	**Status**	**Evidence**
IT Governance	**Defined**	Due to the stringent oversight that this authority is subject to, the organisation has established specific committees who are tasked with ensuring that all stakeholders are aware of there responsibilities in terms of the planning and management of IT. Specific programs have also been implemented to ensure that policies, controls and processes are followed and that intervention and action can be taken in the event of non compliance
IT Strategic Alignment	**Managed and Measurable**	IT planning within the authority is the responsibility of the CIO, however the CIO receives his mandate directly from the senior leadership in the organisation and needs to account for all activities under his control to the political and organisational leadership. Specific strategies and long term planning is conducted to ensure that the organisation has sight of the plans of IT. These plans are subject to review and are communicated to the public to create awareness of the business use of IT to support service delivery.
IT Value Delivery	**Managed and Measurable**	IT within the organisation plays a critical role in supporting the business processes and ensuring that the information which support business operations and decision making is accurate and current. IT is also supporting the delivery of social services to the public and has created a new channel through which the authority can communicate with the public. The management of IT investments is comprehensive and has to be accounted for independently of all other expenditure and investment in order to assess the benefits that are derived from IT services.
IT Risk Management	**Managed and Measurable**	The organisation follows a structured risk management process in order to ensure compliance with government legislation. The controls and systems are subject to independent review and all deficiencies that are highlighted need to be accounted for and rectified in order to prevent future discrepancies. Technology risks are managed in order to ensure that key processes linked to revenue generation and service delivery are not impacted and that appropriate plans are in place to deal with the non availability of systems and services.
IT Performance	**Managed and**	The leadership in the organisation have specific

Management	**Measurable**	performance agreements that are negotiated and review annually in order to ensure delivery. These agreements identify core functions that need to be conducted as well as specific projects and objectives that need to be achieved. Systems monitoring is underpinned by service level agreements in which operating standards and performance targets are established in order to ensure business continuity and efficiency. These target are reviewed monthly and exceptions are discussed and plan are develop to resolve problem areas. The monitoring of systems is also conducted by IT in order to maintain the health of the infrastructure and prevent failure of systems that may impact revenue and transactional services.

Chapter 5

5. Discussion of Findings

In this chapter, the research findings in Chapter 4 are discussed and explained and linked to the research questions.

The public sector adoption of IT Governance processes and controls required to support the delivery of services to constituents, as well as ensuring the availability of business operations was prevalent in all the organisations that responded during this research. However the maturity of the various processes of governance was diverse across specific domains as well as across the various organisations.

Organisations where the focus was specifically related to financial management and economic development had governance practices that were well developed and ensured that IT was able to add value to the overall mandate of the organisation. However in the organisations where social services was the focus, governance processes were limited and not well integrated, as the organisational management was not driving IT initiatives.

The most mature domains in terms of governance practices were strategic alignment and risk management, whereas the maturity of IT performance management was still not sufficiently developed in most organisations in order to take into account the overall service performance and the related processes, systems and skills.

5.1. Review of research questions

What have been the major drivers for ensuring that business and IT are aligned in the public sector?

Due to the impact of industry methodologies such as ITIL and COBIT, public sector organisations have reviewed the role and impact that IT has on the operations in the organisation. These frameworks along with South African initiatives such as the King III report has placed the focus on the leadership in the departments and how they influence the role of IT in their organisations. Two themes that have been consistent throughout this research are the function of formal structures to which IT are accountable as well as the level of the senior IT leader within this organisation.

Based on this research the most common form through which IT and business are able to co-ordinate there respective functions are through committees who are mandated to purely look at the business impact of an IT solution to the business. This structure is supported by the literature (Van Grembergen, 2004; Albrecht and Pirani , 2004; Dahlberg and Kivijarvi, 2006) who all argue that successful alignment is achieved through the formal interaction of business and IT in order to get a common understanding of the goals and objectives of the organisation. This process has many benefits as it allows the business to get an insight into the capabilities and functions of IT in the organisation as well as to understand the impact of new IT projects. IT in response is also able to ensure that the investments that they make into systems are able to improve the overall functioning of the organisation.

What was also evident through this research is that the decision making structures for IT are two tiered. In the first instance business operations are involved in determining the needs of the IT services in the organisation. Business also ensures that IT services that are available to the business are aligned to the functions of each unit and is able to integrate the entire value chain of the organisation. Business is therefore critical in ensuring that IT services that are delivered to the organisation have a direct process improvement result on the function of the organisation and do not impact the users. These decision making structures are representative of the centralised structures identified by Peterson, O'Callaghan and Ribbers, (2000).

Furthermore the role of business leaders in the selection and adoption of IT services in the organisation is important to ensure that the services are accepted by the organisation and that there is minimal resistance to the implementation of services. The fact that business leaders are active in the IT planning process has seen a positive response to accepting IT as a core component of the new way in which government programs will be implemented. The involvement of organisational leaders in IT is seen as the most critical enabling factor to the alignment of business and IT according to Luftman and Brier (1999) and was evident in all of the organisations that respondent.

The fact that organisations are able to understand the capabilities of IT has meant that IT can focus more of there attention of technical matters and ensure that the services and systems that are implemented in the organisation do not disrupt the overall functioning of the organisation.

The level of authority that the senior IT leader has in the department has played a crucial role in the ability of IT to fulfil their mandate. In those organisations where IT were able to communicate directly with the senior leadership within the organisation, the role of IT has been seen as strategic in the development of government programs and are integral in the government's ability to deliver new services to the public. The direct contact that IT enjoys in these organisations also seems to aid the IT entities ability to firstly get business approval for projects that will improve the efficiency of the organisation.

Furthermore the elevation of IT to the highest decision making forums in the organisation has allowed IT to deliver services more effectively and to achieve there objectives. In organisations where IT were accountable to a senior leader who held more than one portfolio there was a level of frustration within the IT leadership to ensure that the projects and plans were communicated effectively to the board as they had to contend with other units who also required the attention and mentorship of the responsible executive. In all these instances it seemed that the IT leadership believes that only through the elevation of IT to the same status as other executive level functions would IT be able to create a platform from which the organisation would be able to take full advantage of the IT services as IT could influence the business planning process and create an awareness of there challenges and collaborate with business in developing solutions to these problem areas.

The role of external stakeholders in the elevation of IT within the organisation also has to be noted. In organisations which were subject to audits based on the requirements of their government mandates, IT

was seen as key in ensuring that effective controls and reports were in place. In these organisations the leadership were intimately involved in the planning and review of IT in the organisation. These can be attributed to the fact that leaders wished to ensure that they were able to ensure that the operations of the organisation was measurable and auditors were able to access evidence fairly easy in order to approve the functions of the organisation.

Due to the renewed focus on accountability and compliance with regulation as indicated by King (2006), there has also been an acceptance of the role of IT in the organisation. The controls and monitoring capabilities that has been embedded within the systems of organisations has meant that business leaders are interested in the function of these services. This has resulted in IT advising the organisation on the measures that can be put in place in order to ensure compliance. In these instances IT has engaged directly with the organisational leadership to ensure that government legislation is adhered to, and that processes can not be manipulated.

The role of IT in controlling fraud as proposed by Damianides (2004) was evident in the strategic planning discussions between the business and IT. On the observations of this research, IT has improved the monitoring of fraudulent activities within public sector institutions. This was seen as essential for government as they have to account for the expenditure of public funds. The credibility that IT has been able to provide to government activities has ensured that government planning now encompasses standards and specifications for systems that are required of all institutions requiring access to government systems. The development of these standards has been driven from business in order to ensure the integrity government processes.

The role of consultants has also positively influenced organisational leadership's perception of IT. In those organisations where external consultants were advising the organisational leadership on their business practices and the impact of IT, the IT leadership has been able to communicate directly with the senior decision makers in the organisation. In these instances the recommendations proposed by consultants has resulted in IT being core to the reconfiguration of business processes. This intervention has allowed the leaders to gain an improved understanding of the critical nature of IT and has seen more senior managers endorsing the initiatives undertaken by the IT organisation.

According to van Grembergen (2004) successful IT and business alignment can also be observed in organisations where projects undertaken by the IT entity are supported by the business leaders. This has in fact been substantiated by the findings in the research, as IT projects that were prioritised based on the programs undertaken by the various institutions were seen as more strategic in nature than in those organisations where IT was viewed as supporting the current operational needs of the organisation.

The final element that has been observed during the research where a strong alignment has been observed between IT and business is in the area of technology driven services. In these instances where IT in itself is the service that is being offered to the public, leaders in these organisations are very interested in the impact that these initiatives will have. IT has resulted in the public having a new medium through which to engage with government and has also being championed as a new revenue stream by organisations that are able to offer communication, collaboration and information services to their constituents. In these instances organisational leaders are involved both in the planning of these services as well as creating an awareness of these initiatives within the organisation as well as to the public by ensuring that they are perceived as championing these schemes. This endorses the view of van Grembergen, (2004), who argues that service delivery can be improved through leveraging IT.

How is the value that is generated from IT within the public environment defined and measured?

The value derived from IT within public sector institutions can be segmented into internal and external value contributions. The areas where IT have added the most value according to this research is through the area of process efficiency and productivity improvements. According to the respondents the role of IT in improving the access to information for the business, has seen more investments being focussed into areas in which organisational processes can be optimised, these findings are line with the research conducted by Tallon, Kraemer and Gurbaxani (1999).

In addition to this the value that IT is able to provide to improving the overall perception of the organisation has been invaluable. The role of IT in improving the integrity, confidentiality and accuracy of information has lead to an overall improvement in the operational effectiveness of the organisation. Due to the impact of IT in these areas the ability of the organisation to counter fraudulent activity and identify information anomalies has contributed to the prominent role that IT now plays in all business processes.

The utilisation of IT has also had a direct process impact in terms of the improve collaboration that it has been able to provide for organisations. The challenge that existed with organisations is that there had not been controls and standards that had been put in place regarding the use of government information. However the use of IT has seen controls and policies being implemented that created a framework for the use of information. These frameworks which are in line with the requirement of the MIOS (2007) have resulted in the centralisation of information as well as reducing the duplication of effort either as a result of lost information or through multiple government entities having to store and interrogate the same information for the same function.

The process impact of IT can also be seen in the improved returns that the public sector has been able to generate by adopting a standard specifications for IT services. The reduction in the number of vendor footprints within and across organisations under the same control has seen government being able to rationalise on the operating costs of the services they provide. Through adopting a standards approach and engaging with vendors to identify strategic partners the public sector institutions have been able to leverage their strong economic position in order to negotiate improved procurement terms based on the volumes that they require and the overall business that government does with the industry. What was prominent throughout this research was the willingness of public sector institutions to take advantage of centralised negotiation and procurement practices which allowed them to benefit from the experienced agencies that procured IT services on government's behalf.

The effect of IT on human capital management within public sector institutions has also contributed to IT value in the public sector. Institutions have adapted to the needs of their personnel to be better informed of there status within these institutions by implementing services that address the government interaction with there employees. Personnel and administrative solutions has made it easier for employees to interact with there organisation and has allowed better career development by ensuring that training and skill developments services move online to allow employees to access educational services.

The communication of operational policies and processes has also been made more accessible to employees and they are more aware of there mandate and the manner in which government expect them to operate. Employees are also better informed of the various regulations under which they operate and are able to make informed decisions that will not jeopardise the organisation's ability to deliver services.

In terms of the external value that IT creates in the public sector, The IT entity in these public sector institutions has seen the transformation of there services from supporting government business to key mechanisms through which government is able to improve the delivery of services to the public. Furthermore IT has also improved the access to government services by previously disadvantaged individuals and remote areas. Based on the input from these respondents it is evident that IT has played a crucial role in supporting the rights of citizens in this country and has also ensured that there is a level of accountability, as proposed by the ITGI (2005b), for the functions provided by government officials, due to the fact that IT has improved information management by ensuring the integrity and reliability of information in the public domain. This was identified as a key function for IT by Hawkins, K.W. Alhajjaj, S and Kelly, S (2003).

The role of IT in improving the relationship between the citizen and the institutions was also seen as key value adds that was provided by IT. In terms of the role IT has played, the contributions can be measured in terms of the increased participation of the public in government initiatives (Di Maio, 2003), as well as in the increase of the public revenue base.

IT has reduced the frustration that is felt by the public by ensuring that services are offered over a channel that requires minimal interaction with a government official. According to various respondents the perception of government officials as being unhelpful and difficult to deal with discouraged many citizens from engaging with government. However through government initiatives such as the Batho Pele program public sector institutions can provide access to there service across internet and mobile platforms.

The value provided by IT to extend government services to under privileged communities has improved the perception of government by the citizen. In an environment where service delivery demands far exceeds the government's capacity to reach all affected parties, IT has allowed government to provide access to social services such as grant distributions in communities where transportation is limited. IT has also ensured that the rights of citizens are defended. The use of IT in this environment has improved the role of government as a protector based on Di Maio's (2003) profile.

Di Maio (2003) had also indicated that IT has improved the role of government as a protector. Based on the research findings, the use of mobile solutions by government has born this point out as

organisations had been able to extend the services of institutions to investigate the abuse of government resources as well as ensure that any violation of the constitution and human rights are investigated by the appropriate resources even though they may not have direct access to the relevant social service.

The role of IT in allowing government to identify trends and isolate problems based on demographic and regional information has improve government planning. Due to the role of IT, government has been able to develop programs and implement the necessary interventions to improve the well being of its citizens.

Di Maio, (2003) also argued that IT Value can be measured in terms of the political return that they were able to achieve. In terms of the political value that IT has been able to add to the public sector, issues such as the impact of IT on improving the implementation of government's manifesto were identified as areas where IT has benefited government. In order to ensure that the investment that the government has committed to social upliftment initiatives are tracked well and to ensure that funds are correctly apportioned and appropriated IT played a critical role. The progress tracking through IT been able to ensure that services and information have become location independent and has allowed organisations to get a real time view of the project which ensures that objectives can be met and that problems can be resolved more promptly.

The Socio-Economic impact of IT in the public sector is another phenomenon that was observed during this study. Issues that can be classified into this area includes skills development, indirect job creation and black economic empowerment. Although these issues may not be considered within most measurements of IT value these elements played a large role during government consideration of IT projects and can be classified as improving government's political return from IT.

In terms of government procurement policies, a focus has been placed on providing opportunities to previously disadvantaged individuals as well as persons with disabilities. This has ensured that government has not only been able to ensure that these individuals are given opportunities within established organisations, who wish to retain the relationships that they have with government, in order to grow there careers. Additionally this policy has seen the emergence of Small and Medium enterprises that are able to provide government will services thereby improving the number of job opportunities available and growing the economy.

With regard to skills development government believes that any investment within the IT environment has to be strongly supported by a direct improvement in the local skills within the country. According to respondents organisations that wanted to provide services, had to be seen as implementing programs to support the local communities. In this manner government was able to achieve a key principle of improving the knowledge base in the country.

A unique perspective that exists within the public sector is the view that public institutions adopt with regard to staff turnover. Based on government's mandate to create job opportunities institutions saw turnover in the environment as positive since they believe that by allowing personnel in the IT environment to move on into better paying positions within the private sector they are not only creating an opportunity for someone else in the public sector but also adding value to the economy by reducing the unemployment rate and the burden on government social services.

The indirect impact of IT on job creation was also a key consideration when considering the value of IT. From a planning point of view the information that is available to decision makers in the organisation which assists them in identifying areas where skills were available and could match available skills to public works programs thereby creating job opportunities within the communities.

The use of technology to improve the overall management of the government supply chain has also contributed to the value delivered by IT. Due to the revitalisation of government procurement processes and policies, business are able to interact and respond to government requests through technology driven channels. These organisations are also able to track the status of there responses and interactions with government ensuring that the processes are more transparent.

The role of IT in ensuring that businesses are also able to hold government accountable to the terms of the business transaction has improved the relationship between government and its vendors as they are able to track all transactions with government from the start.

Vendors are also able to respond to the needs of government more efficiently through technology as they are able to provide the required products or services when they are needed and thereby

eliminating wastage for both parties. This also ensures that government are able to access the required products and services where they are needed in order to provide the end services to their constituents.

What are the key components of the IT risk management program within the public sector?

The IT risk management framework that has evolved within public institutions is very well aligned with the overall business risk framework in these organisations. Government institutions are well aware of the stringent legislative framework under which they operate as well as the specific regulations that dictate there interaction with both suppliers and information users. The process through which risk within the IT entity is managed are driven from the executive level, as the organisational processes are highly depended on automation for ensuring that they are able to achieve there mandate. Regardless of the fact of whether IT was seen as an enabling, transformational or a support function in the business, risk management was integral to the overall management of IT in these organisations.

The process of developing the risk management framework for IT involved both the business and IT, and can be delineated into business risks and technical risk. In terms of the business risk, the business managers in the organisation were responsible for ensuring that they were able to identify the key dependencies that the organisation had on IT and what the impact it would have if these services or information was not available.

IT together with the business was responsible for ensuring that specific plans were in place to ensure that those dependencies that the business identified which they believed were essential to ensure continuous service delivery were mitigated against. Secondly a plan was developed to ensure that critical services were available in the event that the business was subject to a disaster. In those organisations where a comprehensive plan was in place IT services were replicated to locations which would ensure that the organisation was still able to communicate with their stakeholders and provide essential information and transactional services to there constituents.

A final element of the business risk plans was the management of information and the usage of organisational assets which played a key role within the context of legal risks. This was an area that was very well developed and there were comprehensive policies that had been put in place in order to

ensure that information that was critical to the functioning of the organisation was protected and stored. The tracking of users within the online environment was also stringently policed to ensure there information in the organisation was not compromised. This area was also a key budget priority for most of the respondents and the securing of the organisation's assets and information was an area where executives were also able to involve themselves within the IT operations.

In terms of the technical risks that existed in this environment two major categories were identified, these were architectural and systems risks.

In terms of architectural risk the IT leadership were responsible for ensuring that all development within there environment was able to meet the business objectives for which they were undertaken. It was essential that these were closely monitored as they could have a financial or operational impact on the business. These risks were assessed in terms of there accuracy of achieving business objectives, as well as their compatibility and integration into the existing environments.

The systems risk perspective that was identified addressed questions related to the system operation. Within this framework issues such as internal and external threats that could result in service disruption were addressed. In terms of the key area that was focussed on IT were concerned about the issue of viruses and malicious software that could impact on the information processing and communication capabilities of there institutions. Policies were developed and enforced through the utilisation of automated solutions to ensure that services were protected. IT was also proactive in developing surveillance capabilities to ensure that they were able to detect and react to a threat. Relationships with external parties were also emphasised in order to ensure that the right skills and knowledge was available to inform and assist the organisation of impending danger to the operations.

In order to mitigate against a system failure two principles were key. In the first instance it was essential that the organisation was able to carry out routine maintenance on there systems in order to ensure that all elements of the system were up to date and that any component where a potential failure was identified was highlighted to the senior management and plans were developed to resolve these issues. IT was also responsible for ensuring that there were limited single points of failure that could prevent service delivery. In order to prevent this critical systems were always developed with redundancy and seamless failover to ensure that in the worst case services may be degraded but never unavailable.

How is the performance of IT within the government assessed?

The common trend that was observed across all respondents was a strong correlation between the strategic objectives of the organisation and the performance measurements of the overall IT entity within the organisation. Furthermore the capacity to support the growing needs of the business and the ability to adapt IT to the operational environment were also observed. There were also internal performance measurements within the IT entity that were used to assess the contribution of IT services as well as to assess the involvement of individual resources within the IT environment.

The performance objectives of the overall IT department which are measured within the overall performance management system of the organisations were generally based on formalised contracts. The respondents all indicated that the process through which the IT function is assessed can be segmented into annual and perpetual objectives.

The annual objectives are linked to the key objectives that the organisation wishes to achieve and are related to the key projects that will be undertaken by IT in order to support the business. Through this process, priorities were established based on a negotiation process with the executives, and targets agreed based on the ability to achieve these targets. The targets were set based on the criticality of the projects to the overall success of a government project, as well as the impact that it would have on the business. The senior IT leadership were then responsible for decomposing these targets into specific objectives for the personnel within the IT environment in order to ensure that various functions with IT are able to collaborate and ensure that the common goals are achieved.

Perpetual performance contracts for IT were based upon the competency areas within IT and can be further segmented into technology management, process management and vendor management. The performance measurements were articulated into quantitative measures and were based upon predefined standards and metrics which would ensure that the business was able to achieve its service delivery goals. The trend within these organisations was to adopt a performance charter which was then underpinned by internal service level agreements through which IT could be assessed.

In terms of technology management it is the responsibility of the IT leadership to agree and communicate to the business the level at which they expect their systems and services to perform. The

most common attributes of these measures were systems availability that was measured in terms of the uptime of the systems as well as the number of times when the services were inaccessible. These measures were considered critical to the perception of the IT service to the business and were constantly monitored by the leadership in order to identify areas where interventions was urgently required in order to improve standards.

Process measurement for the IT department was based on the ability of the IT department to handle specific queries from users. The main measurement criteria in this environment was how many problems and faults were attended to within a predefined time and to ensure a level of competency within the IT department which was able to handle the issue in a professional manner. The leadership in IT used these measurements to ensure that processes that required improvement were identified and that weaknesses and skills gaps were identified and programs put in place to resolve these issues.

Due to the critical and confidential nature of the information that the institutions handled, it was imperative that measures were put in place to ensure that the IT entity managed this well. The measures that were essential in this environment were the integrity, reliability and accuracy of the information that was to be used by the business. These measures were essential to ensure that the organisation was able to provide and effective service to the public as well as to ensure that the reputation of the institution is not compromised due to information being accessed or made available to unauthorised individuals. It also ensured that a level of trust and confidence could be placed in the processes of the organisation as the manipulation of information was made difficult while at the same time allowing transparency in terms of the legislative framework in the country.

Based on the finding of the research a domain checklist has been developed. These checklists indicate the most critical principles, derived from the literature, and a responsibilities and process guideline, derived from the findings, which have been implemented in the responding organisations. The principles, responsibilities and processes indicated in the tables below were the most prevalent in the research conducted and the responses provided during the interview process.

Table 16: Domain Principles and Implementation Guidelines

Domain	Principles IT Strategic Alignment
Principles	IT investment aligned with strategic objectives IT operations are aligned with enterprise operations IT strategy supports enterprise strategy Business Leadership provide guidance to IT Leadership are the principal sponsors of IT in the organisation Business and IT management are represented on IT committees Business and IT jointly define role of IT in the organisation Governance addresses the architecture and process requirements that IT systems implement to support the business Governance ensure priority for IT projects and systems Governance ensure that service agreements are developed for critical IT services
Responsibilities	Establish an oversight board to assess the impact of IT in the organisation Steering committees need to be in place to assess the impact on business operations and objectives Appoint and Executive to head IT that is directly accountable to the board for IT investment and performance Project Committees need to be appointed who are responsible for ensuring successful implementation of IT projects Develop Procurement and Supply Chain Management Channels that can evaluate the total cost and capabilities of a proposal Develop an IT charter to support business objectives
Processes	Adopt a industry best practices to provide guidance Establish a Framework that indicates the role of the business and the duties of the IT unit Understand and Implement the recommendations of the King III report Develop formal planning and reporting forums and timelines Develop Policies that control the responsibilities and duties of all IT stakeholders Ensure that Technology Projects are communicated in terms of organisational outcomes and improvements Review IT plans and processes and ensure they are mapped to business process and outcomes

Domain	IT Value Delivery
Principles	Deliverables achieve the benefits that were promised Deliverables provide appropriate quality Deliverables are on-time Deliverables are within-budget Standards are derived from business requirements Do policies provide deliverables What are the depend variables of value management
Responsibilities	Develop specific delivery unit within IT to address Projects, Development and Support Ensure that IT has skills to assess the total economic value of a solution Develop a framework to identify and assess the impact of IT on organisational objectives as well as the improved interaction with the public Ensure standard specifications are developed to improve the sharing of information Understand the human impact of IT interventions and develop appropriate change management programs Develop appropriate training and communication programs to ensure acceptance of IT
Processes	Assess IT solution based on the total cost Evaluate the impact of IT on improving departmental Service Delivery Evaluate the impact of IT on improving departmental Operational Efficiency Evaluate the impact of IT on improving departmental Political Objectives Develop a full requirement of the business requirement and solution Ensure that Project are continuously assessed and in line with business expectations Communicate the capabilities and function of the IT services and processes to the organisation

Domain	IT Risk Management
Principles	Formally acknowledge that the risk exists and monitor it Implement controls to mitigate against risks Share risk with partners or transfer to insurance coverage Ensure compliance with regulatory requirements Ensure Compliance with contractual requirements Ensure compliance with standards and specifications IT systems provide controls that ensure transparency and eliminate wastage, fraud and process manipulation Information controls are clearly defined and protect the organisation information from unauthorised access and abuse
Responsibilities	Ensure that IT risk is part of overall organisational risk planning Identify risks to systems and process Link risks to business processes are prioritise them based on their impact Define Business and technical Risks Develop appropriate risk plans Understand legislation that control business processes and information management and ensure that policies are developed to encompass these Ensure that systems are compliant with legislation and allow for improved business transparency and reporting
Processes	Establish a forum to oversee the risk management process Interact with internal and external auditors to identify non compliance Continuously monitor IT environment and track systems and processes active in the organisation Identify systems or processes that are not in line with organisation policies and implement remedial plans Establish contract with vendors to ensure compliance with licensing agreements and operating procedures Develop business continuity as well as operational availability plans Ensure that critical information is protected and stored in the event of loss or damage

Domain	IT Performance Management
Principles	Define clear goals and good measures that unequivocally reflect the business impact of IT goals
Responsibilities	Establish Targets for Systems and Processes and constantly monitor these to identify deviations Negotiate service levels and response times with business Implement systems to monitor the performance of systems Conduct regular formalised feedback sessions with business and process owners Develop performance agreement for all IT personnel that are linked to business outcomes Identify areas where skills are required and develop an appropriate training plan Establish annual and perpetual performance targets for IT resources.
Processes	Establish a tracking system to monitor the all issues raised with IT Establish Service Level Agreements with user departments and Vendors

5.2. Conclusion

With regard to the traditional locus of IT decision-making authority the participants interviewed all played key roles directing the architecture, process frameworks and policy development within the IT discipline in there organisations.

It was also found that IT within the participating organisations was a key focus area for executives during formal reporting and communication forums. There was a perception amongst the respondents that the executives in these organisations were not fully aware of the overall potential and capabilities that existed within the IT environment, but believed that IT had the potential to transform these organisations. It was also found that in organisations where IT played a key transformational role there was a close interaction between the executive management team and the IT executives. In these instances the IT executives were part of the top decision making structures in the organisations.

The role of resources both systems and personnel in achieving the objectives of the IT department was also seen as a key element by the respondents. The respondents believed that the knowledge and career development of the IT personnel was critical in ensuring that the perception of IT within the organisation changed and that IT was viewed as a key participant in the achievement of the organisational objectives.

The investment in systems that supported the organisational process was also critical to the perception of IT in the organisation. In those instances where IT systems were reliable and continuously available the perception from executives was that IT could play a key role in the transformation and ability of the organisation to achieve its mandate.

Chapter 6

6. Conclusion

6.1. Introduction

This chapter discusses the overall results of the research and identifies key outcomes of the overall function of IT in the public sector along with the governance practices which supports the IT function within the government sector. The overall attainments of the research objectives are also reviewed and the limitations of the research as well as recommendations to management are highlighted.

6.2. Main Findings of the research

The emphasis within the public sector to redress the inequalities of the past has compelled public sector institutions to review their business processes as well as the systems that support them. The focus has resulted in IT being viewed as a key component of all government initiative to deliver services to their constituents. Furthermore due to the ability of IT to deliver immediate returns in terms of service improvements public sector institutions have investment substantially in systems and processes which can improve the access to government services.

However in terms of governance there is still a large disparity between the management and control of IT within public sector institutions. In those organisations where financial and information services are the core business processes, governance initiatives are quite advanced and many of these organisations have adopted practices that have been successfully implemented within the private sector.

The main drivers for the adoption of IT Governance within these public sector institutions was to ensure that IT was seen as a reliable and dependable service through which services could be delivered to the public. IT Governance also played a key role in ensuring that systems were in place whereby government objectives and programs could be adequately monitored and provided feedback to the relevant implementation units in order to resolve problems when they occurred.

The principle of institutionalising the values of government was also a key consideration for IT in terms of the governance initiatives as it ensured that roles and responsibilities were defined and also ensure that there ware improved collaboration between various organisations within government in order to deliver services.

In terms of improving the alignment between the objectives of the business and IT within the public sector, organisations have also begun adopting a more systematic approach to there planning and decision making processes. The elevation of the senior IT personnel within the public sector was evident in most of these organisations. This elevation has allowed IT to gain a better understanding of the overall mandate of the organisation. In many of the organisations the maturity of the strategic alignment was evident and has seen IT develop comprehensive plans that were associated with specific business process and could be measured against specific business outcomes. The introduction of governance guidelines such as the King II and King III reports was a catalyst for many executives to understand there responsibilities as far as IT was concerned especially as no specific public sector guideline existed to guide organisational leaders in the public sector.

The commitment of the senior leadership in many organisations where IT was seen as a key delivery mechanism was also observed in this research. The executives in these organisations were intimately involved in ensuring that IT was able to support the business objectives. The key mechanism through which many of the executives engaged with IT was through the establishment of IT steering committees who were responsible for driving the implementation of IT programs that could benefit the organisations overall functions.

In terms of the value of IT within the public sector, a persuasive argument can be made for the role and function of IT identified in the literature and the public sector adhering to these guidelines. From a value perspective IT played both a critical role internally in improving efficiencies, as well as to the public by providing access to government services. Although many of the organisations had adopted the approach of proposing solutions to the organisations based on the service delivery benefits that could be derived from IT, there was no evidence to suggest that any model had been adopted to monitor the continued benefits that can be derived from IT initiatives in the long term. Many of the organisations still justified the value of the IT expenditure of financial measures but the implementation of metrics to measure

political objectives and service delivery objectives were purely based on project post mortems and is a key area that would need further investigation.

The public sector institutions were well aware of their various legislative and regulatory obligations, as well as the need to ensure compliance with government operating standards. In terms of ensuring this compliance IT were well positioned by working with the overall governance and risk structures within there respective organisations in order to ensure that the systems were compliant. In most instances risk management was the area where there was effective communication and collaboration with internal stakeholders in order to ensure that IT did not compromise the overall rating of the organisation. From a systems perspective risk was still seen on in terms of access control, service continuity and information security. There was also evidence to suggest that a complete IT risk plan had been put in place is the larger organisations to cover system, processes and resources.

The performance management area seemed to be the area where development still needed to be done. Many of the organisations had implemented processes that could provide them with information on the overall performance of the systems, but an integrated framework still needed to be developed to account for the total value derived from IT and the performance of the IT entity in the organisation.

6.3. Recommendations for Management

In order to ensure that IT is able to deliver value to public sector institutions, the primary recommendation of this research is that public sector institution on the whole revisit the overall mandate that is given to the IT entity within there organisations. Furthermore the senior leaders within the organisation need to take a key role in championing the programs that are undertaken by IT in order to improve the acceptance throughout the organisation. The adoption of guiding frameworks such as COBIT as well as by experts such as van Grenbergen (2004) and Weill (1997) will improve the co ordination and collaboration between the organisations and its IT arm.

Furthermore in terms of risk and performance management framework that the organisations adopt it is recommended that management consider the overall services and not just the specific elements. An IT service consists of system, processes and resources that support it. In order to assess the overall risk to the business organisations need to identify plans for each element of the service and assess its impact on the organisation. Similarly in terms of performance management if the service is assessed holistically the organisation will be able to identify areas that require improvement and ensure that specific programs are in place to ensure continuous optimisation of these services.

6.4. Suggestion for further Research

Throughout the research process it became evident that the development of a framework to ensure that governance practices adopted by public sector institutions were able to ensure that IT generates value was required. In terms of the literature most of the focus has been on implementing IT Governance structures within the corporate environment. IT would therefore better assist public sector organisations if the processes and responsibilities identified during this research could be validated and key deliverables and success criteria defined for each domain from a public sector perspective.

Furthermore the approach adopted for this research was to assess the views of people that operated within the IT environment. In order to develop an overall assessment of the role of governance and the value of IT in the public sector additional investigations would need to be conducted with all stakeholder groups. This research would have the benefit of understanding the perception of IT from the organisational and well as the citizen's perspective.

Additionally the area that was identified as the most underdeveloped from an overall maturity perspective was performance management. Additional research would need to be conducted to determine in this was the case and what interventions could be undertaken to improve this situation.

Appendix A: Consistency Matrix

Problem	Research Questions	References	Test Instrument
Role of IT Governance in delivering Business Value	What have been the major drivers for ensuring that business and IT are aligned in the public sector?	Gantin, 2006; ITGI, 2005b; King 2006; Mercury, 2006b; Sharif, 2006	Cognitive mapping
	How is the value that is generated from IT within the public environment defined and measured?	Albrecht, P. and Pirani, J.A. 2004; Di Maio, A. (2003); Bernroider, E.W. and Hampel, A. 2005; Broadbent, M. and Weill, P. 1993; Gerrard, M. 2005; ITGI 2005b	Cognitive mapping
	What are the key components of the IT risk management program within the public sector?	ITGI, 2007; Peterson, 2000; Broadbent, M. and Weill, P. 1997 van Grembergen, 2004	Cognitive mapping
	How is the performance of IT within the government assessed?	Gerrard, M. 2005; Peterson, 2000; Van Grembergen, 2004	Cognitive mapping

Appendix B: Interview List

Land Bank
Gauteng Shared Services Centre
Ekhuruleni Municipality
Statistics SA
Department of Land Affairs
Industrial Development Corporation
South African Reserve Bank
SAPO
Public Investment Corporation
Auditor General
Independent Development Trust
South African Weather Services
South African Human Rights Commission
South African Social Services Agency
South African Local Government Agency

Appendix C: Interview Questions

1. What do you believe is the function of IT Governance in the organisation?

2. How are IT Governance structures organised within the business? Can you describe the channel and structures that have been established to coordinate the activities of IT Governance?

3. What structures are in place to confirm that IT/business architecture is designed to drive maximum business value from IT?

4. What processes and practices have been put in place to ensure that IT delivers provable value to the business?

5. How is the value contribution of IT measured and appropriately managed?

6. What role do the board, line managers and IT management play in IT risk and value management?

7. What role does risk and value management play in during the IT planning process?

8. How does the business ensure that IT assets and investments are actively managed over their complete lifecycle?

9. How successful has IT Governance been is ensuring that requests for information and assistance from business units been?

10. How do you ensure that the organisation adheres to regulatory requirements and best practices?

Appendix D: COBIT Maturity Matrix

Source: Control Objectives for Information Technology, IT Governance Institute (2007)

	IT Governance
Non Existent	There is a complete lack of any recognisable IT Governance process. The organisation does not even recognise that there is an issue to be addressed; hence, there is no communication about the issue.
Ad Hoc	There is recognition that IT Governance issues exist and need to be addressed. There are *ad hoc* approaches applied on an individual or case-by-case basis. Management's approach is reactive, and there is only sporadic, inconsistent communication on issues and approaches to address them. Management has only an approximate indication of how IT contributes to business performance. Management only reactively responds to an incident that has caused some loss or embarrassment to the organisation.
Repeatable	There is awareness of IT Governance issues. IT Governance activities and performance indicators, which include IT planning, delivery and monitoring processes, are under development. Selected IT processes are identified for improvement based on individuals' decisions. Management identifies basic IT Governance measurements and assessment methods and techniques; however, the process is not adopted across the organisation. Communication on governance standards and responsibilities is left to the individual. Individuals drive the governance processes within various IT projects and processes. The processes, tools and metrics to measure IT Governance are limited and may not be used to their full capacity due to a lack of expertise in their functionality
Defined	The importance of and need for IT Governance are understood by management and communicated to the organisation. A baseline set of IT Governance indicators is developed where linkages between outcome measures and performance indicators are defined and documented. Procedures are standardised and documented. Management communicates standardised procedures, and training is established. Tools are identified to assist with overseeing IT Governance. Dashboards are defined as part of the IT balanced business scorecard. However, it is left to the individual to get training, follow the standards and apply them. Processes may be monitored, but deviations, while mostly being acted upon by individual initiative, are unlikely to be detected by management.
Managed and Measurable	There is full understanding of IT Governance issues at all levels. There is a clear understanding of who the customer is, and responsibilities are defined and monitored through SLAs. Responsibilities are clear and process ownership is established. IT processes and IT Governance are aligned with and integrated into the business and the IT strategy. Improvement in IT processes is based primarily upon a quantitative understanding, and it is possible to monitor and measure compliance with procedures and process metrics. All process stakeholders are aware of risks, the importance of IT and the opportunities it can offer. Management defines tolerances under which processes must operate. There is limited, primarily tactical, use of technology, based on mature techniques and enforced standard tools. IT Governance has been integrated into strategic and operational planning and monitoring processes. Performance indicators over all IT Governance activities are being recorded and tracked, leading to enterprise wide improvements. Overall accountability of key process performance is clear, and management is rewarded based on key performance measures.
Optimised	There is an advanced and forward-looking understanding of IT Governance issues and solutions. Training and communication are supported by leading-edge concepts and techniques. Processes are refined to a level of industry good practice, based on results of continuous improvement and maturity modelling with other organisations. The implementation of IT policies leads to an organisation, people and processes that are quick to adapt and fully support IT Governance requirements. All problems and deviations are root cause analysed, and efficient action is expediently identified and initiated. IT is used in an extensive, integrated and optimised manner to automate the workflow and provide tools to improve quality and effectiveness. The risks and returns of the IT processes are defined, balanced and communicated across the enterprise. External experts are leveraged and benchmarks are used for guidance. Monitoring, self-assessment and communication about governance expectations are pervasive within the organisation, and there is optimal use of technology to support measurement, analysis, communication and training. Enterprise governance and IT Governance are strategically linked, leveraging technology and human and financial resources to increase the competitive advantage of the enterprise. IT Governance activities are integrated with the enterprise governance process.

Source: Control Objectives for Information Technology, IT Governance Institute (2007)

	IT Strategic Alignment
Non Existent	IT strategic planning is not performed. There is no management awareness that IT strategic planning is needed to support business goals.
Ad Hoc	The need for IT strategic planning is known by IT management. IT planning is performed on an as-needed basis in response to a specific business requirement. IT strategic planning is occasionally discussed at IT management meetings. The alignment of business requirements, applications and technology takes place reactively rather than by an organisationwide strategy. The strategic risk position is identified informally on a project-by-project basis.
Repeatable	IT strategic planning is shared with business management on an as-needed basis. Updating of the IT plans occurs in response to requests by management. Strategic decisions are driven on a project-by-project basis without consistency with an overall organisation strategy. The risks and user benefits of major strategic decisions are recognised in an intuitive way.
Defined	A policy defines when and how to perform IT strategic planning. IT strategic planning follows a structured approach that is documented and known to all staff. The IT planning process is reasonably sound and ensures that appropriate planning is likely to be performed. However, discretion is given to individual managers with respect to implementation of the process, and there are no procedures to examine the process. The overall IT strategy includes a consistent definition of risks that the organisation is willing to take as an innovator or follower. The IT financial, technical and human resources strategies increasingly influence the acquisition of new products and technologies. IT strategic planning is discussed at business management meetings.
Managed and Measurable	IT strategic planning is standard practice and exceptions would be noticed by management. IT strategic planning is a defined management function with senior-level responsibilities. Management is able to monitor the IT strategic planning process, make informed decisions based on it and measure its effectiveness. Both short-range and long-range IT planning occurs and is cascaded down into the organisation, with updates done as needed. The IT strategy and organisationwide strategy are increasingly becoming more co-ordinated by addressing business processes and value-added capabilities and leveraging the use of applications and technologies through business process re-engineering. There is a well-defined process for determining the usage of internal and external resources required in system development and operations.
Optimised	IT strategic planning is a documented, living process; is continuously considered in business goal setting; and results in discernible business value through investments in IT. Risk and value-added considerations are continuously updated in the IT strategic planning process. Realistic long-range IT plans are developed and constantly updated to reflect changing technology and business-related developments. Benchmarking against well-understood and reliable industry norms takes place and is integrated with the strategy formulation process. The strategic plan includes how new technology developments can drive the creation of new business capabilities and improve the competitive advantage of the organisation.

Source: IT Enterprise Value: Governance of IT Investments The Val IT Framework, IT Governance Institute (2005a)

	IT Value Delivery
Non Existent	The enterprise sees the IT function as a supplier and a cost to be minimised. There is limited communication between the business and the IT function.
Ad Hoc	The enterprise recognises that IT is both a cost and an investment. There is increasing communication between IT and the other business functions about the need to demonstrate return on IT investments. Accountabilities are not defined beyond the level of delivering technical capabilities. Reporting is budget- and cost-driven. Business cases are defined on a project by-project basis and often are incomplete. Skills and tools exist on an individual, *ad hoc* basis.
Repeatable	There is increasing awareness amongst business and IT management of the need for a more formalised governance framework. The business and IT functions are working more collaboratively on the need to demonstrate the return on IT enabled investments. Some individuals take ownership for the realisation of benefits, but there is no formal commitment from the business. Business cases and investment status reports are required for most investments, and there is some limited reporting on benefits. On-the-job training is provided in business case development on an as-needed basis. Tools are increasingly used in response to *ad hoc* needs, but are not standardised across the enterprise.
Defined	The business and IT functions understand the governance requirements to select and execute new investments, deliver the resulting IT services efficiently, and ensure optimal allocation of IT resources. Business cases, including benefits realisation plans, and status reporting are required for all investments. The IT function and business users share the accountability for implementing programmes, and for benefits realisation, but roles and responsibilities are unclear. Formal training plans exist but are not consistently executed. Tools are increasingly used to support comparable evaluation of investments, but are still not standardised across the enterprise.
Managed and Measurable	There is a shared commitment between the business and the IT function to optimise the contribution of individual IT investments and services to business value. Accountability for achieving the business benefits is clearly assigned to the business functions. Business cases are reviewed, updated and re-evaluated throughout the full life cycle of investments.Processes and skills exist to support investment decision making and value management, and to ensure that resource allocation is consistent with the priorities. Standard tools, integrated with other enterprise systems, are adopted and formal training plans are executed.
Optimised	Value management is part of the corporate culture. The business and IT functions work in partnership to continually optimise and report on the portfolios of IT investments, and resulting services, assets, and other resources. Accountability for optimising business value from the overall portfolio is clearly assigned and monitored. Processes are continuously improved. External expertise is called on to benchmark and challenge investment assumptions. Tools provide comprehensive reporting, including succinct, all-around reviews of the performance of the portfolio, and include analytical capabilities.

Source: Control Objectives for Information Technology, IT Governance Institute (2007)

	IT Risk Management
Non Existent	Risk assessment for processes and business decisions does not occur. The organisation does not consider the business impacts associated with security vulnerabilities and development project uncertainties. Risk management is not identified as relevant to acquiring IT solutions and delivering IT services.
Ad Hoc	IT risks are considered in an *ad hoc* manner. Informal assessments of project risk take place as determined by each project. Risk assessments are sometimes identified in a project plan but are rarely assigned to specific managers. Specific IT-related risks, such as security, availability and integrity, are occasionally considered on a project-by-project basis. IT-related risks affecting day-to-day operations are seldom discussed at management meetings. Where risks have been considered, mitigation is inconsistent. There is an emerging understanding that IT risks are important and need to be considered.
Repeatable	A developing risk assessment approach exists and is implemented at the discretion of the project managers. The risk management is usually at a high level and is typically applied only to major projects or in response to problems. Risk mitigation processes are starting to be implemented where risks are identified.
Defined	An organisation wide risk management policy defines when and how to conduct risk assessments. Risk management follows a defined process that is documented. Risk management training is available to all staff members. Decisions to follow the risk management process and receive training are left to the individual's discretion. The methodology for the assessment of risk is convincing and sound and ensures that key risks to the business are identified. A process to mitigate key risks is usually instituted once the risks are identified. Job descriptions consider risk management responsibilities.
Managed and Measurable	The assessment and management of risk are standard procedures. Exceptions to the risk management process are reported to IT management. IT risk management is a senior management-level responsibility. Risk is assessed and mitigated at the individual project level and also regularly with regard to the overall IT operation. Management is advised on changes in the business and IT environment that could significantly affect the IT-related risk scenarios. Management is able to monitor the risk position and make informed decisions regarding the exposure it is willing to accept. All identified risks have a nominated owner, and senior management and IT management determine the levels of risk that the organisation will tolerate. IT management develops standard measures for assessing risk and defining risk/return ratios. Management budgets for an operational risk management project to reassess risks on a regular basis. A risk management database is established, and part of the risk management processes is beginning to be automated. IT management considers risk mitigation strategies.
Optimised	Risk management develops to the stage where a structured, organisation wide process is enforced and well managed. Good practices are applied across the entire organisation. The capture, analysis and reporting of risk management data are highly automated. Guidance is drawn from leaders in the field, and the IT organisation takes part in peer groups to exchange experiences. Risk management is truly integrated into all business and IT operations, is well accepted and extensively involves the users of IT services. Management detects and acts when major IT operational and investment decisions are made without consideration of the risk management plan. Management continually assesses risk mitigation strategies.

Source: Control Objectives for Information Technology, IT Governance Institute (2007)

	IT Performance Management
Non Existent	The organisation has no monitoring process implemented. IT does not independently perform monitoring of projects or processes Useful, timely and accurate reports are not available. The need for clearly understood process objectives is not recognised.
Ad Hoc	Management recognises a need to collect and assess information about monitoring processes. Standard collection and assessment processes have not been identified. Monitoring is implemented and metrics are chosen on a case-by-case basis, according to the needs of specific IT projects and processes. Monitoring is generally implemented reactively to an incident that has caused some loss or embarrassment to the organisation. The accounting function monitors basic financial measures for IT.
Repeatable	Basic measurements to be monitored are identified. Collection and assessment methods and techniques exist, but the processes are not adopted across the entire organisation. Interpretation of monitoring results is based on the expertise of key individuals. Limited tools are chosen and implemented for gathering information, but the gathering is not based on a planned approach.
Defined	Management communicates and institutes standard monitoring processes. Educational and training programmes for monitoring are implemented. A formalised knowledge base of historical performance information is developed. Assessment is still performed at the individual IT process and project level and is not integrated amongst all processes. Tools for monitoring IT processes and service levels are defined. Measurements of the contribution of the information services function to the performance of the organisation are defined, using traditional financial and operational criteria. IT-specific performance measurements, non-financial measurements, strategic measurements, customer satisfaction measurements and service levels are defined. A framework is defined for measuring performance.
Managed and Measurable	Management defines the tolerances under which processes must operate. Reporting of monitoring results is being standardised and normalised. There is integration of metrics across all IT projects and processes. The IT organisation's management reporting systems are formalised. Automated tools are integrated and leveraged organisation wide to collect and monitor operational information on applications, systems and processes. Management is able to evaluate performance based on agreed-upon criteria approved by stakeholders. Measurements of the IT function align with organisation wide goals.
Optimised	A continuous quality improvement process is developed for updating organisation wide monitoring standards and policies and incorporating industry good practices. All monitoring processes are optimised and support organisation wide objectives. Business driven metrics are routinely used to measure performance and are integrated into strategic assessment frameworks, such as the IT balanced scorecard. Process monitoring and ongoing redesign are consistent with organisation wide business process improvement plans. Benchmarking against industry and key competitors becomes formalised, with well-understood comparison criteria.

Reference List

Ahmad, R and Ali, N.A. (2003): The use of cognitive mapping technique in management research, Management Research News; Volume26, Number 7

Albrecht, P. and Pirani, J.A. (2004): Using an IT Governance Structure to Achieve Alignment at the University of Cincinnati, EDUCAUSE Centre for Applied Research, Boulder Colorado, pp 1-18

Ackermann, F. and Cropper, S. (1992): Geeting Started with Cognitive maps. Yuoung OR Conference, University of Warwick, April 1992

Atkinson, J. and Leandri, S. (2005): Best Practices: Organisational Structures that support compliance, Finacial Executive, pp 36-40

Bai R (2003), Organisational factors influencing the quality of IS/IT strategic planning process, Industrial Management and Data Systems, Volume 103 Number 8, pp 622-632

Bakker, B. (2006): IT Governance is empowering the board, iWeek, issue 63, 17 August 2006, pp 25-29

Bandyopadhyay. K, Mykytyn. PP, Mykytyn. K (1999): A framework for integrated risk management in information technology, Management Decisions, Volume 37 Number 5, pp 437-444, MCB University Press

Benbasat, I., and Zmud, R. W. (1999). Empirical research in information systems: The practice of relevance. MIS Quarterly, Volume 23, Number 1,pp 3-17.

Bernroider, E.W. and Hampel, A. (2005): Enterprise Resource Planning And IT Governance in Perspective: Strategic Planning and Alignment, Value Delivery and Controlloing, The Fifth International Conference on Electronic Business

Bimrose, J, Barnes. S and Brown. J (2005): A Systematic Literature Review of Research into Career-related Interventions for Higher Education; Institute for Employment Research, University of Warwick

Borland (2006): IT Maqnagement and governance, February 2006, pp 1-26

Boudreau, M. ,Gefen, D. and Straub, D.W. (2001): Validation in Information Systems Research: A State of the Art Assesment, MIS Quarterly, March 2001, pp 1 -16

Brink, H.I. (2001): Fundamentals of research methodology for health care professionals. Cape Town, Juta and Company

Broadbent, M. and Weill, P. (1993): Improving Business and Information Strategy Alignment: Learning from the Banking Industry, IBM Systems Journal, Volume 32 No. 1, pp 162-179

Broadbent, M. and Weill, P. (1997): Management by Maxim: How Business and IT Managers Can Create IT Infrastrucutres, Sloan Management review, Spring 1997, Volume 38 no. 3, pp77 -91

Burns, T. (2001): Implications of Information Technology on Corporate governance, International Journal of Law and Information Technology, Volume 9 No.1, pp 21-38

Calder, A. and Watkins, S (2005): IT Governance A Manager's Guide to Information Security and BS 7799/ISO 17799, Kogan Page, London

Chan, Y. (2000): IT Value: The Great Divide Between Qualitative and Quatitative and Individual Organisational Measures, Journal of Management Information Systems, Spring 2000, Volume 16 no. 4, pp 225-261

Chan, Y. Huff, S.L. Barclay, D.W. and Copeland, D.G. (2001): Business Strategic Orientation, Information Systems Strategic Orientation, and Strategic Alignment, Information Systems Research, Volume 8 no.8, June 1997

Choudrie, J and Dwivedi, Y.K. (2005): Investigating the Research Approaches for Examining Technology Adoption Issues, Journal of Research Practice, Volume 1, Issues 1, pp 1-12

Cliffe Dekker (2008): Commentary on the Electronic Communications and Transactions Act, 2002,
http://www.cliffedekker-hofmeyr.com/files/Cliffe_Dekker_Commentary_ECT_Act.pdf
Accessed (8 October 2008)

Coupe, G (1995): Information Technology: Grasping at governance, StandardView, September 1995, Volume 3 No.3, pp 107-111
Crowther, D (1996): from the foundation upwards: evaluating business performance, Managerial Auditing Journal, 11(1), 35-47

Cronk, M. and Fitzgerald E.P. (2002): Constructing a Theory of 'IS Business Value' from the Literature, Electronic Journal of Business Research Methods, Volume 1 Issue 1, pp 11-17

Dahlberg, T. and Kivijärvi, H. (2006): An Integrated Framework for IT Governance and the Development and Validation of an Assessment Instrument, Proceedings of the 39th Hawaii International Conference on System Sciences

Damianides, M. (2005): Sarbanes-Oxley and IT Governance: New Guidance on IT Control and Compliance, Information Systems Management, Winter 2005, Volume 22 No. 1, pp 77-85

Davies P, (2004): Information systems evaluation and the information systems development process, The Journal of Enterprise Information Management, Volume 17 Number 4, pp 276-282.

Dietrich, R. (2004): S-Ox and the Need to Audit IT Processes, Sarbanes-Oxley Journal,

Di Maio. A, (2003a): Value for Money not Enough in Public Sector IT Projects, Gartner Research, June 2003

Di Maio. A, (2003a): How to Measure the Public Value of IT, , Gartner Research, June 2003

Falconer. D.J. , and Mackay. D. R. , (1999): The Key to the mixed Methods Dilemma; Tenth Australasian Conference on Information Systems; pp 286 - 297

Feeny, D.F. Edwards, B.R. Simpson, K.M. (1992): Understanding the CEO/CIO Relationship, MIS Quarterly, Volume 16 No. 4, December 1992, pp 435-448

Fujitsu Systems (2006): IT Governance – The Future of Control, pp 2-7

Galliers, R. D., and Land, F. F. (1987): Choosing an appropriate information systems research methodology. Communications of the ACM, Volume 30 Number 11, pp900 - 902.

Gantin, J (2006): Assessment of IT Value Delivery at a Large Nordic Bank; Master Thesis Stockholm, Sweden 2006

Gerber. M, and von Solms. R (2005): Management of risk in the information age; Computers and Security; Issue 24, pp 16 -30

Gerrard, M. (2005): Business/IT Alignment a Crtical Factor When Determining IT's Role, Gartner Research, October 2005

Gerrard, M. (2006a): Defining IT Governance: Roles and Relationships, Gartner Research, October 2006

Gerrard, M. (2006b): Defining IT Governance: The Gartner IT Governance Demand/Supply Model, Gartner Research, October 2006

Glazier, D. (2006): Managers determine IT's role
http://www.itweb.co.za/sections/business/2006/0607311405.asp , Accessed November 2006

Glazier, D. (2006): Staff buy-in crucial to IT Governance
http://www.itweb.co.za/sections/business/2006/0607271400.asp , Accessed November 2006

Hamel, G. and Prahalad, C.K. (1989): Strategic Intent, Harvard Business Review, May – June 1990 pp 63-76

Hawkins, K.W. Alhajjaj, S and Kelly, S (2003): Using CoBIT to Secure Information Assets, The Journal of Government Financial Management, Summer 2003, Volume 52 No. 2, pp 23-31

IT Governance Institute (2007): Control Objectives for Information Technology, Rolling Meadows, Illinois.

IT Governance Institute (2005a): IT Control Objectives for Sarbanes-Oxley, Brussels, Belgium.

IT Governance Institute (2005b): IT Enterprise Value: governance of IT Investments The Val IT Framework, Brussels, Belgium.

Jackson, K.M. and Trochim, W.M.K. (2002): Concept Mapping as an Alternative Approach for the Analysis of Open-Ended Survey Responses, Organisational Research Methods, Vol. 5 No. 4, October 2002 307-336

Jasperson, J.S., Carte, T.A., Saunders, C.S., Butler, B.S., Croes, H.J.P., and Zheng, W. (2002): Power and information technology research: A metatriangulation review. MIS Quarterly volume 26, Number 4, 2002, pp 397--459.

Joseph Martin, C.F. (2006): Aligning Manufacturing Information Systems with Business Strategy: A Practical framework, http://www.itgi.org/Template.cfm?Section=HomeandCONTENTID=5558andTEMPLATE=/ContentManagement/ContentDisplay.cfm, Accessed December 2006

Kelle, U. (1998): Computer-Aided Qualitative Data Analysis, Sage Publications, London

King, M. (2001): King report on Corporate Governance for South Africa 2001; http://www.ukzn.ac.za/ukznms/king-report-on-corp-gov.pdf ,Accessed 10 October 2008.

King, M. (2006): The Corporate Citizen: governance for all entities, Penguin Books, Johannesburg

Kotane (2008): Municipal Finance Management Act; http://moseskotane.gov.za/documents/policies/mfma.html accessed 15 December 2008

Krippendorff, K. (1980): Content analysis. An Introduction to its Methodology. Beverly Hills: Sage.

Kurien, P. Rahman, W. and Purushottam (2004): The Case for Re-examining IT effectiveness, The Journal of Business Strategy, Volume 25 no. 2, pp 29-36

Levy, Y. and Ellis, T.J. (2006): A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research, Informing Science Journal, Volume 9, 2006, pp 181-212

Luftman, J. and Brier, T. (1999): Achieving and Sustaining Business-IT Alignment, California Management Review, Volume 42 No.1, Fall 1999, pp 109-122

Marx, F.E. (2003) E-commerce – The effect of the electronic communications and transactions act 25 of 2002 on E-commerce; proceeding from the 5th Annual Conference on World Wide Web Application, September 2003,

Mawson, M. (2006): Companies resist IT Governance, http://www.itweb.co.za/sections/computing/2007/0702070900.asp, Accessed November 2006

Mayring, P (2000): Qualitative Content Analysis; Qualitative Social Research Forum, Volume 1 (2), June 2000

Mercury (2006a): Sustainable Compliance: IT Governance Challenges and Best Practices, Mercury Research,

Mercury (2006b): Optimize IT Governance: Optimize the Business Outcome of IT, Mercury Research,

Mercury (2006c): Six IT Governance Questions Executives Should be Asking, Mercury Research,

Michalsons (2008): Guide to the ECT Act http://www.irmsa.org.za/library/iforest/Michalsons%20Infosheet%20-%20Guide%20to%20the%20ECT%20Act.pdf , Accessed (8 October 2008)

Miles, M.B. and Huberman, M.A, (1994): Qualitative Data Analysis, Sage Publications, London

Miller, G. and Dingwall, R. (1997): Context and Method in Qualitative Research, Sage Publications, London

Miller, M. and Riechert, B.P. (1994): Identifying Themes via Concept Mapping: A New Method of Content Analysis, Theory and Methodology Division, Association for Education in Journalism and Mass Communication Annual Meeting

Mingers. J, (2001): Combining IS a research method: Towards a pluralist methodology, Information Systems Research; Volume 12, Number 3, September 2001; pp240 – 259

Mooney, G.J. , V Gurbaxani. V. , Kraemer. K. L. , (1995): A Process Oriented Framework for Assessing the Business Value of Information Technology; Proceedings of the Sixteenth Annual International Conference on Information
Systems: Amsterdam, The Netherlands, December 1995, pp 17-27.

Novak, J.D. and Canas, A.J. (2006): The Theory Underlying Concept Maps and How to Construct Them, Florida Institute for Human and Machine Cognition, http://cmap.ihmc.us/Publications/ResearchPapers/TheoryCmaps/TheoryUnderlyingConceptMaps.htm, Accessed December 2006.

Oetitinger, A.G. and LeGates, J.C.B. (2000): Holistic framework for IT Governance, Harvard University, Cambridge, Massachusetts

Olzak, T. (2008): A Practical Approach to Managing Information Systems Risk

Ozen, U. and Ulengin F. (2001): Analyzing Strategic thoughts of corporations based on cognitive maps; Proceeding from The19th International Conference of The System Dynamics Society, July 227, 2001; Emory Hotel and Conference Center ,Atlanta, Georgia, USA

Peterson, R. R. (2000). Emerging capabilities for IT Governance: Exploring stakeholder perspectives in Financial Services. *Conference Proceedings European Conference on Information Systems 2000*, *Vienna*, *Austria.*

Peterson, R. R. (2001). Configurations and coordination for global information governance: Complex designs in a transnational European context. *Proceedings of the 34th HICSS Conference*, *Hawaii.*

Peterson, R. R. (2004): Crafting Information Technology governance, Information Systems Management, Fall 2004, Volume 21 No.4, pp 7-22

Peterson, R.R. O'Callaghan and Ribbers, P.M.A. (2000): Information Technology governance by design: Investigating Hybrid Configurations and Integration Mechanisms, pp 435-452

Pinsonneault. A, and Kraemer. K: (2006): Survey Research Methodology in Management Information Systems: An Assessment**,** Accessed 24 March 2006 http://www.crito.uci.edu/research-archives/pdf/urb-022.pdf.

Porter, M.E. (1985) Competitive Advantage: Creating and Sustaining Superior Performance, The Free Press, MacMillan Incoprporated, New York

Powell. E.T (2006): Analysisng Qualitative Data, Accessed 1 April 2006, http://s142412519.onlinehome.us/uw/pdfs/G3658_12.PDF

Pultorak, D. and Keerigan, J. (2005): Conformance, Performance and Rapport: A Framework for Corporate and IT Governance, Directors Monthly, February 2005, pp 15-19

Rasmussen. M, (2006): Taking Control of IT Risk; Forrester Research

Rau, K.G.(2004): Effective governance of IT: Design Objectives, Roles and Relationships, Information Systems Management Fall 2004, Volume 21 No. 4, pp 35-42

Renken, J. (2004): Developing an IS/ICT Management Capability Maturity Framework, Proceedings of SAICSIT 2004, pp 53-62

Robbins S (2004): IS governance, Information Systems Management, Fall 2004, Volume 21 No.4, pp 81

Salle, M (2004): IT Service Management and IT Governance Review, Comparative Analysis and their Impact on Utility Computing, Hewlett- Packard, pp 1-25

Sambamurthy, V. and Zmud, R. (1999): Arrangements for Information Technology governance: A Theory of Multiple Contigincies: MIS Quarterly, Volume 23 No. 2, June 1999, pp 261-290

Senge, P.M. (1990): The Fifth Discipline: The Art and Practice of the Learning Organisation, Doubleday, New York

Senne, D (2006): Slow IT Governance Implementation
http://www.itweb.co.za/sections/business/2006/0607281301.asp , Accessed November 2006

Setsoto (2008): Public Finance Management Act – PFMA, http://www.setsoto.co.za/PFMA.html, accessed 15 December 2008

Sharif, A.M. (2006): realizing the Business benefit of enterprise IT, Handbook of Business Strategy, pp 347-350

Siau, K. and Tan X (2008): Use of Cognitive Mapping Techniques in Information Systems Development, The Journal of Computer Information Systems, Volume 48, Number 4, Summer 2008, pp 49 - 56

Simonsson, M. and Johnson, P. (2006): Assessment of IT Governance: A Prioritization of Cobit, KTH Royal Institute of Technology, Stockholm Sweden

Symons, C. (2005): IT Governance Framework, Forrester Research, March 2005

Tallon, P.P. Kraemer, K.L. and Gurbaxani, V. (1999): A Value-Based Assessment of the Contribution of Information Technology to Firm Performance, Center for Research on Information Technology and Organizations, Graduate School of Management, University of California, Working Paper, August 1999

Tan, F.B. and Gallupe, R.B. (2006): Aligning Business and Information Systems Thinking: A Cognitive Approach, IEEE Transactions on Engineering Management, Volume. 53, Number. 2, May 2006, pp 223-237

Tavakolian, H. (1989): Linking Information Technology Structure with Organisational Competative Strategy: A Survey, MIS Quarterly, September 1989, pp 309 – 317

Tyler, D. (2001): Cognitive mapping: A tool to support strategic management, Journal of Fashion Marketing and Management, Volume. 5, Number 4, pp 353 -357

Van Grembergen, W. (2004): Strategies for Information Technology governance, Ideas Group, London

Waterhouse, P. (2006): IT Governance – An Integrated Framework and Roadmap: How to Plan Deploy and Sustain fo Competative Advantage, Computer Associates White Paper.

Weil, P. And Ross, J. (2004). Don't Just Lead, Govern: How Top-Performing Firms Govern IT. http://mitsloan.mit.edu/cisr/rpapers.php (accessed 15 March 2007)

Weill, P. and Ross, J. (2005): A Matrixed Approach to designing IT Governance, MIT Sloan Management Review, Winter 2005, pp 25 – 34

Weill, P. Subramani, M. Broadbent, M (2002): Building IT Infrastructure for Strategic Agility, MIT Sloan Management Review, Fall 2002, pp 57 – 65

Zorn, T. (2008): Designing and Conducting Semi-Structured Interviews for Research, Waikato Management School
http://www.pua.edu.eg/Version2/Courses2/Business/Freshmen/MGT101/Slides/Interviewguidelines.pdf(accessed 3 October 2008)