Mitigating Risk Through Effective Information Technology Operations in Local Governments - Towards a Best Practice

by

Emile Kaselowski

Mitigating Risk Through Effective Information Technology Operations in Local Governments - Towards a Best Practice

by

Emile Kaselowski

Dissertation

submitted in fulfillment
of the requirements
for the degree

Magister Technologiae

in

Information Technology

in the

Faculty of Engineering, the Built Environment and Information Technology

of the

Nelson Mandela Metropolitan University

Supervisor: Professor Rossouw von Solms

January 2008

Declaration

I, Emile Kaselowski, hereby declare that:

- The work in this dissertation is my own work.
- All sources used or referred to have been documented and recognised.
- This dissertation has not previously been submitted in full or partial fulfillment of the requirements for an equivalent or higher qualification at any other recognised educational institution.

Emile Kaselowski

Abstract

Sound IT governance is becoming increasingly important for any public or private organisation. However, based on previous research, it can be argued that local municipalities in South Africa are seemingly struggling to implement sound IT governance practices. As a result, very few municipalities perform strategic IT planning and as many as 80% of municipalities do not have a Master System Plan (MSP) in place, which is required by law. IT governance and corporate governance are lately viewed as one and no longer as two separate governance disciplines, because computer systems and electronic communication are more important now than ever for the survival of any organisation. Therefore, it is important for municipalities to streamline their efforts towards sound IT governance. There are limitations which are faced by municipalities that limit these efforts. Possibly the biggest contributing factor towards this current municipal IT governance predicament, among others, is the fact that there are very few, if any, guidelines and resources available to municipalities to aid them in implementing proper IT infrastructures, systems and governance procedures. To improve the current state of IT governance in municipalities, better guidelines and procedures are required.

This dissertation presents an IT governance framework to meet this afore-mentioned requirement. It is tailored to the requirements of local municipalities and is based on the international best practice, the Control Objectives for Information and related Technologies (COBIT) and the ISO/IEC 17799 code of practice for information security management. This proposed framework takes into account the Municipal Systems Act (nr 32 of 2000), Municipal Structures Act (nr 117 of 1998) and annual municipal IT audit reports' requirements.

Research was conducted at a district and its underlying, local municipalities to determine the proper IT governance criteria for municipalities. Case studies were performed at the municipalities and consisted of performing literature studies on the available municipal legislation and annual, municipal IT audit reports, conducting COBIT gap analyses, an ISO 17799 analysis, conducting interviews and developing questionnaires and data capturing and presentation tools.

The resultant, proposed IT governance framework, titled the IT strategic objective plan (IT-SOP), when implemented by a municipality, should provide a solid governance foundation on which to base its business processes on.

Acknowledgements

I would like to thank the following:

- My supervisor, Professor Rossouw von Solms for the time, valuable insight and guidance that he provided without which this dissertation would not have been possible.
- My family, I appreciate the encouragement and all forms of assistance
- The financial assistance of the National Research Foundation (NRF) is hereby acknowledged. Opinions expressed and conclusions arrived at are those of the author and are not necessarily attributed to the NRF.

Contents

List of Figures

List of Tables

Part I

Introduction

Chapter 1

Introduction

1.1 Background

Corporate governance practices in South Africa have received much attention since the publication of the King II report on good corporate governance in 2002, at which time it was heralded as the leader in corporate governance guidelines. This report has since been accepted by government as the *de facto* standard of governance principles. Although King II has established a "serious concern" for better corporate governance methods in South Africa, the organisational community should continue to implement and improve corporate governance structures "in order to keep up with the rest of the international business world." (Ernst and Young, 2004).

The King II report includes a number of topics that are relevant to this project. These are firstly, that it is applicable to public sector organisations, such as local governments (district and local municipalities) (Cliffe Dekker, 2002a). Secondly, the board of an organisation is ultimately responsible for the affairs of that organisation, and each member can personally be held accountable and liable for any financial irregularities. Thirdly, the board shall be responsible for identifying risk areas and performance indicators in respect of the organisation. (Cliffe Dekker, 2002b)

In today's age of technology, it is an accepted fact that information technology (IT) can make or break an organisation, depending on how it is implemented and governed. With many financial and information systems currently in use at municipalities, as well as the legislation mentioned above, it can be seen that IT assets have to be properly governed in order to combat fraud and to protect the board, as well as the overall organisation.

IT governance and corporate governance can no longer be seen as two different disciplines, according to the Information Technology Governance Institute (ITGI) (Gamma, 2007). Therefore, IT is no longer only a "technical issue", with the responsibility lying with an employee lower down in the organisational hierarchy. Rather, IT has developed into a "horizontal" function, spanning across every business function within the organisation. Therefore, IT governance has grown to be very important in any organisation and the IT function within an organisation preferably also needs a voice at board-level.

International standards have also been developed regarding the topic of IT governance within organisations. Two of these are the ISO/IEC 17799 (also known as BS7799 or ISO 27002 lately) standard dealing more specifically with information security and assurance and COBIT, from the Information Technology Governance Institute (ITGI), dealing with IT governance.

1.2 Description of Problem Area

For any organisation, such as a local government, to be well governed, it must incorporate and base its operating strategy on best practices (IT Governance Institute, 2000b). Instead, few, if any, standards exist for the governance of IT within local governments. As a result, information technology has been neglected and kept at a low profile. Thus, the huge potential benefits that IT can provide are left unutilized. There are, however, the Municipal Finance Management Act (IMFO, 2003) and the Municipal Systems Act (Government Gazette, 2000) that prescribe, to a certain degree, the role of IT systems and risk management within local governments.

Currently, there is a requirement for a practical IT governance framework to aid in the development and management of IT in local governments, amongst other requirements and problems. These other problems include: the lack of skills and knowledge of IT in municipalities, unsatisfactory reporting lines between the IT function and the rest of the organisation, no collaboration and coordination relationships between local governments and the disposition of IT departments within local governments, all causing information technology to ultimately be misaligned with the business objectives of local governments.

Based on research done by ForgeAhead, a leading South African research company that focuses on the development of IT within government, 284 local governments participated in a study regarding Information Technology governance. In the report that was released in March 2005, it was found that about 80% of municipalities do not have a Master System Plan (MSP) for the implementation of information technology (IT) infrastructure (Mochiko, 2005a). Other findings from the study were that local governments lack a funding procedure, skills and that they do not know the IT sector and its policies (Mochiko, 2005a). No other studies could be found that are similar to the research project described in this dissertation.

Very few municipalities in South Africa have an MSP in place and are struggling to implement an efficient IT infrastructure that will enhance service delivery to its customers, according to Mochiko (2005a). However, very little published guidelines, literature and other resources exist that can be used by a municipality to aid the development of governance procedures and processes that will ensure the development of such an IT infrastructure.

1.3 Research Questions

Currently, hardly any governance standards and procedures exist for the governance of IT within local governments. There is a lack of a practical and understandable best practice to ensure the effective governance of the IT asset in local governments. Thus, the IT asset is not ideally aligned with municipal business objectives.

The primary research question for this dissertation is: “How can COBIT be tailored into a best practice IT governance framework to suit the requirements of local municipalities in South Africa that will ensure that the IT infrastructure and systems are aligned with the municipal objectives, provide sufficient risk and threat mitigation, enable local governments to coordinate and collaborate on strategic planning and overall IT governance?”

The problem requires decomposition into smaller sub-problems to accurately address these issues. These sub-problems are:

- Which COBIT high-level control objectives are applicable to the business processes of a local municipality?
- What are the current maturity levels for each of the applicable control objectives, measured against COBIT’s maturity model?
- What are the acceptable maturity levels for each of the applicable control objectives, measured against COBIT’s maturity model?
- Which of the applicable objectives are more important than others?
- How can the ISO 17799 code of practice for information security management be used to complement the IT governance framework which is based on COBIT and which of the ISO 17799 security controls are applicable to a local municipality?

1.4 Objectives

The primary objective of this research project is to draft a best practice framework to effectively mitigate Information Technology-related risks in local governments and to provide an effective service to both internally-related governance issues and externally-related service delivery.

A number of secondary objectives need to be accomplished to achieve the primary objective. These are:

- Developing a base framework that contains the control objectives from COBIT that are applicable to a local municipality;
- Combining the ISO 17799 security controls with the COBIT objectives and analysing which of these security controls are applicable to a local municipality;
- Defining a project plan that will ensure that the IT governance framework is successfully implemented in a local municipality.

1.5 Research Philosophy

It is important to understand the research philosophy of a research project, because it provides the reader with a certain viewpoint of how the project should be interpreted. This should ensure that the reader, when examining the project, is aware of what to expect from the project, including the scope and possible limitations.

This research project mainly involves information systems. This means that it also involves people in some or other way. Whenever people are involved in a system such as an information system, it forms part of some social phenomena. Thus, the focus of research is more on what is being researched, rather than on the actual measurement. This research project is therefore more qualitative that results in a predominantly interpretive-oriented or phenomenological research philosophy.

1.6 Research Methodology

The research methods used in this research project are literature studies, case studies, questionnaires, interviews and arguments. An extensive literature study was conducted to identify relevant national and municipal legislative and regulatory issues. Also, IT governance best practices (specifically COBIT and ISO 17799) as well as other governance mandates was researched, e.g., the King II report.

By means of case studies in typical local governments, gap analyses was performed at the individual municipalities, in the form of case studies, to identify the true situation of IT governance in different local governments against internationally accepted best practices such as COBIT. These case studies made use of interviews, questionnaires, and in-depth literature studies of the annual, municipal IT audit reports. The results from the case studies were compared to identify similarities and differences within the IT governance processes and structures of the participating municipalities. The annual, municipal IT audit reports of the various municipalities were then further investigated, compared and analyzed for similarities and differences in order to identify compliance and regulatory issues that were relevant to local governments. An ISO 17799 analysis was then conducted to determine which ISO 17799 information security controls were applicable to a local municipality and were required to be implemented. This analysis was also conducted in the form of a case study, making use of interviews and questionnaires. Based on the results from the literature survey, gap analyses, investigation case studies, ISO 17799 analysis and auditing requirements, the information technology governance framework (an IT strategic objective plan) was proposed and motivated, through sound arguments.

1.7 Layout

The dissertation consists of seven chapters. **Chapter 1**, this chapter, presents the subject area of the study, the principal research question and further highlights how this question is addressed. Hereafter, **Chapter 2** discusses the concepts of corporate governance and information technology (IT) governance and how these two concepts are currently considered as a single, integrated, corporate governance discipline. Sound corporate and IT governance are critical to the well-being of any organisation and therefore, the focus of **Chapter 3** is to narrow down the scope of corporate and IT governance to district and local governments. The function of this chapter is to state the research problem and highlight the various constraints and current problems of IT governance in local municipalities. **Chapter 4** is the beginning of the solution section of the dissertation. This chapter discusses all the factors which had an influence on the project, as well as explains the research methodology that was used to conduct the COBIT case studies. The anatomy of the project, case studies and their deliverables and outcomes are then discussed. **Chapter 5** discusses the COBIT case studies and the ISO 17799 analysis in detail, focusing on the COBIT gap analysis questionnaires as well as the tool that was developed to compute the results and provide the required gap analysis and objective priority information. The COBIT gap analysis was performed to determine the applicable objectives, as well as their levels of implementation which are acceptable. This chapter further discusses the ISO 17799 analysis which was conducted at the district municipality. This analysis was performed to determine the relevancy of the ISO 17799 controls to a municipality. The information from the COBIT gap analysis and the ISO 17799 analysis were used to define the IT governance framework in the form of the IT Strategic Objective Plan (IT-SOP), which is discussed in **Chapter 6**. This chapter explains how all of the information from the case studies and ISO 17799 analysis was mapped, combined, prioritised and grouped into phases in order to produce the IT-SOP. The chapter further examines the project plan that was developed to complement the implementation of the IT-SOP, which contains the necessary tasks, objectives and milestones to ensure that the IT-SOP is successfully implemented by the municipality. **Chapter 7** discusses the reasons why the IT-SOP can be further developed into a best practice, as well as summarizes the dissertation, highlights the final conclusions and presents the further research opportunities. Figure 1.1 depicts the layout of the dissertation.

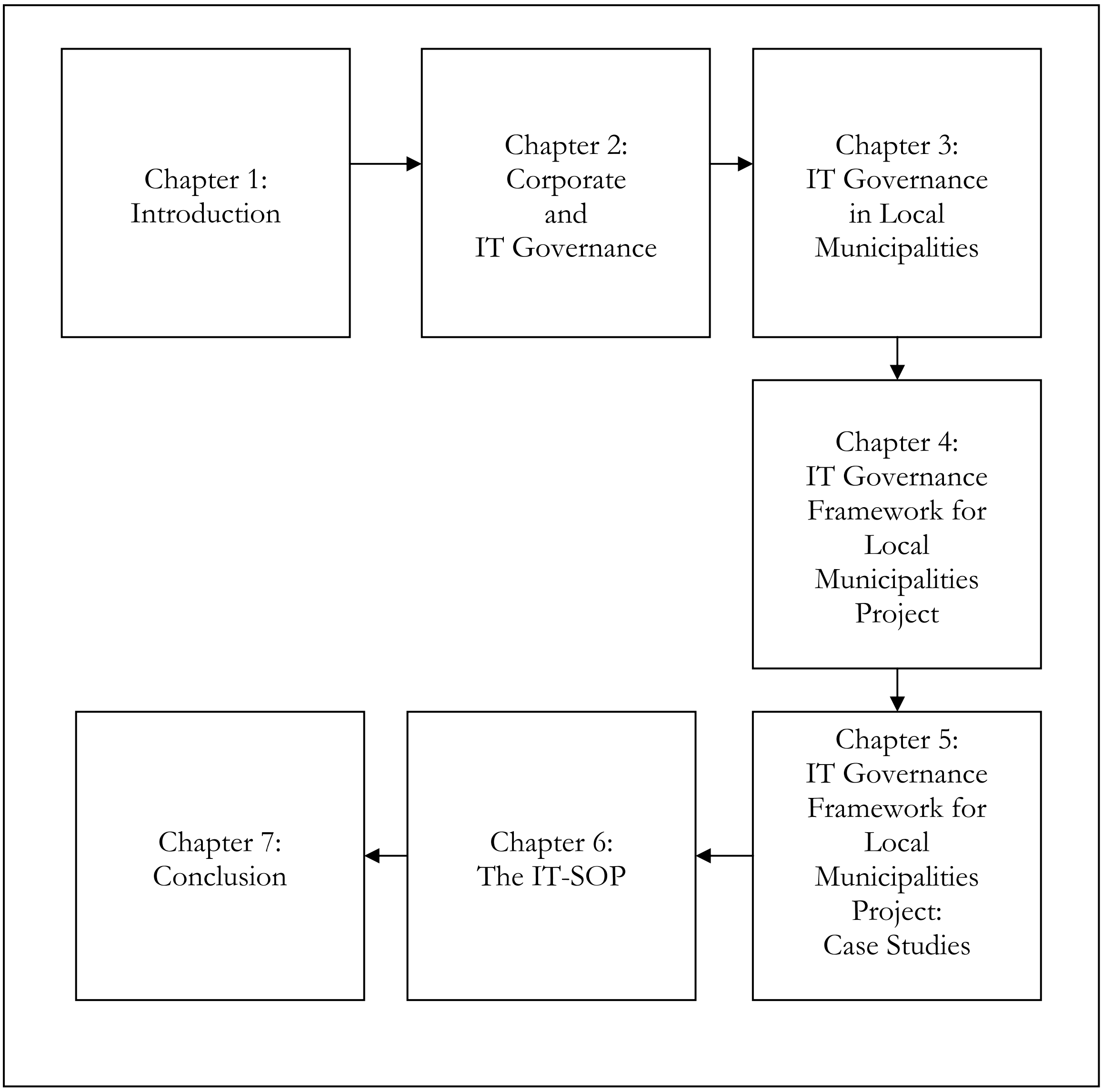


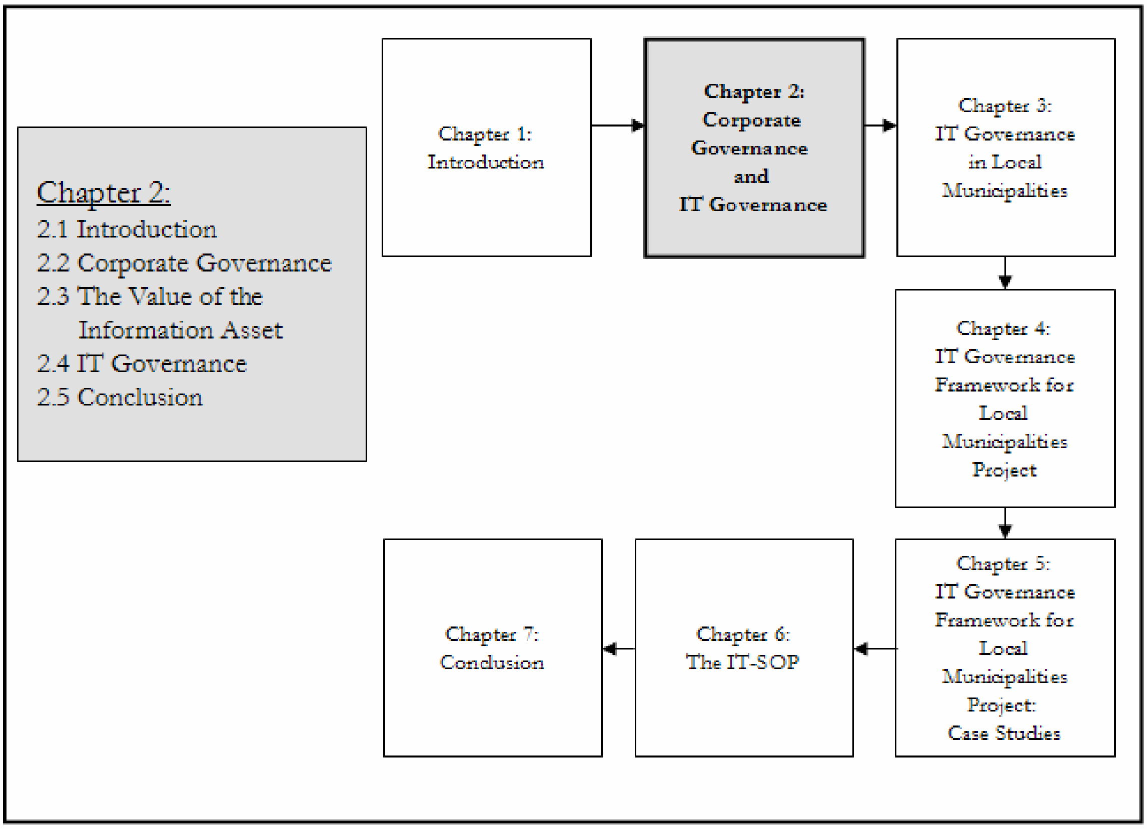
Figure 1.1: Proposed Layout of the Dissertation

Part II

Background

Chapter 2

Corporate and IT Governance


Chapter 2:
2.1 Introduction
2.2 Corporate Governance
2.3 The Value of the Information Asset
2.4 IT Governance
2.5 Conclusion
Chapter 1: Introduction
Chapter 2: Corporate Governance and IT Governance
Chapter 3: IT Governance in Local Municipalities
Chapter 4: IT Governance Framework for Local Municipalities Project
Chapter 5: IT Governance Framework for Local Municipalities Project: Case Studies
Chapter 6: The IT-SOP
Chapter 7: Conclusion

2.1 Introduction

Corporate governance provides the organisation with the structure through which objectives are set, the means of attaining those objectives and how the performance is measured (Cadbury, 1992). Poor corporate governance can have extremely negative effects on any organisation (Tarimo, 2006). Various causes for poor corporate governance can be identified, albeit fraudulent or unintentional actions. Possibly the biggest contributing factor towards poor corporate governance within an organisation is the quality and management of the information assets on which business-critical decisions are taken. If the information assets are not protected properly, then critical decisions might be based on information which has little value. These ill-informed decisions are risky and often have disastrous outcomes. The lack of sound corporate governance principles in organisations such as WorldCom and Enron have been stated as the major cause for accounting fraud and poor organisational performance (Ramaswamy, 2005). These organisations were forced to close down and financial losses to shareholders and employees were substantial.

In this chapter, the link between corporate governance and information technology (IT) governance is explored. Using the literature available, corporate governance is defined, and in order to better understand it, its objectives and features are briefly discussed. The need to improve it is explored, and some examples are given of companies which have experienced the effects of poor governance practices. The importance of information and its reliance on IT are then briefly discussed. Best practices which can be implemented to contribute towards better corporate governance within an organisation are also discussed. This chapter is concluded by describing the formal link between corporate governance and IT governance.

2.2 Corporate Governance

Sound corporate governance is vital for organisations to remain competitive (Centre for Business Research, 2004). Too many corporate and financial fraud cases, of which WorldCom, Enron and Parmalat (Ramaswamy, 2005) are a few famous examples, have been seen in the past. These cases were directly related to poor corporate governance and have caused much concern among investors (Ramaswamy, 2005). To better understand this concept, some background, objectives and strategies of corporate governance need to be discussed.

In order to protect investors, various new laws, practices and regulations have recently been published which define the implementation of better governance principles and techniques

(Loyd, 2004). Both the Sarbanes-Oxley Act in the United States and the King II Report in South Africa are examples of such laws and practices. Since then, board executives and CEOs worldwide have since started to investigate their companies' internal governance practices for fear of being found guilty of negligence, thus perhaps facing prison terms for violating these corporate governance mandates (Changepoint Corporation, 2004). However, a tendency has developed where organisations address their corporate governance practices merely for annual reporting purposes, thus addressing corporate disclosure as an end in itself out of fear of noncompliance (Ryan, 2007). Corporate governance addresses much more than just corporate disclosure and compliance. Other issues, such as the effectiveness and efficiency of operations and the safeguarding of assets also form part of effective corporate governance strategies (CPA Audit, 2007). It is therefore important to understand the full meaning of corporate governance in order to implement sound corporate governance practices within an organisation.

Corporate governance can be defined as the system by which an organisation or company is directed and controlled in order to achieve its objectives (CPA Audit, 2007). This system provides the mechanics for the organisation to operate effectively and efficiently towards its organisational objectives. It also provides the foundation and structures on which organisational rules and policies are developed, which conduct is acceptable and what is not acceptable and how the organisational performance and compliance is monitored and measured. Good corporate governance enables the organisation to set its objectives, as well as to provide assurance to all interested parties that these objectives have been achieved. The Queensland Government (2002) stated that good corporate governance is the "glue" between the organisation and its objectives. Without good corporate governance, there is very little assurance that an organisation will function as it intends to do.

2.2.1 Aspects of Corporate Governance

The main objective of corporate governance is to enhance the well-being of any organisation by providing it with the following four key governance aspects (Kurkure, 2006). The first aspect which it provides is strategic vision. An organisation which is well governed provides for the development of objectives and strategic, long and short range plans for how to achieve the objectives. The second aspect it provides is predictable operations and outcomes. This predictability feature also institutes investor trust. Transparency is the third aspect provided by good corporate governance. It enables the organisation and its interested parties, investors and employees to know exactly what the status of the organisation currently is and it ensures that fraudulent activities cannot occur undetected. The fourth and last aspect provided by good corporate governance is accountability. Accountability mechanisms ensure that there is an entity, such as a person or department, which is responsible for every process or operation of the organisation. These aspects in their totality contribute to better stakeholder satisfaction, since it can be ensured that the organisation is properly governed.

2.2.2 The Need for Good Corporate Governance

After the collapse of WorldCom and Enron, investors have become careful when assessing which companies to potentially invest in. As a result, investors now say that they would pay more for shares of a well-governed organisation than a poorly governed one (McKinsey, 2007). Good corporate governance can thus be considered a hallmark of quality to outsiders and potential investors. As such, it has also become a necessity to be able to remain competitive in global markets (Loyd, 2004). Therefore, the better an organisation is governed, the more shareholder activity can be expected since good governance, regulatory and legislative compliance strengthens investor and stakeholder trust.

If an organisation is to survive, it should ensure the highest levels of investor trust as possible; therefore, it should make an ever-increasing effort towards better corporate governance.

2.2.3 Examples of Bad Corporate Governance

Various companies have experienced the effects of bad corporate governance practices.
Internationally, Enron, WorldCom and Parmalat serve as a few examples of companies which were victims of corporate and accounting fraud (GURN, 2006). In South Africa, companies such as Crusader Life, AA Mutual, Cape Investment Bank and Alpha Bank failed because of bad management decisions, which indirectly relates to poor corporate governance (Ryan, 2007).

These failures could have been prevented if these companies had adopted the kind of corporate governance structures which are becoming increasingly commonplace around the world (Ryan, 2007). By definition, corporate governance is not only concerned with preventing accounting fraud, but with the way in which the whole organisation is governed, including decision-making. There is increasing evidence that collaborative decision-making greatly reduces the risk of business failure.

It is therefore obvious that any organisation should adopt good corporate governance principles in its organisational structure and processes in order to survive and be successful.

2.2.4 Concluding Corporate Governance

Good corporate governance is essential for any organisation to survive. Not only does it ensure that the organisation is efficient and effective in working towards its goals, but it serves as a hallmark of quality for investors and other stakeholders to strengthen trust relationships between the organisation and its internal and external parties.

As indicated in the introduction, many organisations have failed as a result of poor corporate governance. This section discussed what is meant by good corporate governance and how it strengthens stakeholder and organisational trust.

In the previous sub-section it has been highlighted that effective decision-making is core to good corporate governance. As most decisions are based on current, reliable information it is important to ensure quality information. In order to understand how information and the governance of information and its related technologies can contribute towards better corporate governance, the value of information and why it is important is discussed next.

2.3 The Value of the Information Assets

Thompson and von Solms (2005) describe information as “a fundamental asset within any organisation”. To fully comprehend the importance of information, Botha and von Solms (2001) state that information is the life-blood in any organisation. It would be very difficult to govern an organisation without the correct information readily available. As businesses and organisations grow larger and information is stored in various mediums, it becomes increasingly difficult to govern the usage and storage of information.

Information can be classified as some form of knowledge that is exchanged, and is represented by some form of data (Oasis, 2002). Information is represented within the organisation as anything ranging from financial reports, supplier lists, project plans and anything else which can provide strategic value to the organisation. Information is, however, exposed to various threats which can render it useless. Therefore, measures should be implemented to ensure that information is always available to authorised users, current, correct and in a usable format.

In order to better manage organisational information, companies turned to Information Technology (IT) to process, store, transport and present information. Companies have since begun to experience the many advantages of implementing IT solutions to manage their information. IT has become so popular that, according to Keen (1991), it has "reshaped the basics of business." Various business processes, strategies and other entities have since relied heavily, or are entirely based on IT.

IT has advanced rapidly during the last few decades. Many organisations have made the shift towards implementing IT as a business-enabling technology and to create value for the organization. Initially, computer terminals were used to capture and present information to the business. These computers were connected to a large, central mainframe computer where all the information and data were stored and processed. Input and output were very basic, with punch cards being used primarily for the input of instructions into the computer (Perry, Schneider, 2001). Governing the technology was simple, since access could be restricted with the use of physical security mechanisms.

Smaller, faster and smarter computers came into existence as well as faster and more reliable networking technologies. These technologies proved to be cost effective, as well as more efficient and much more affordable. Governance of these technologies became more difficult, but all the data and information were still contained within company boundaries. Devices continued to advance and became smaller and more affordable, while increasing in the variety of features, speed and efficiency. Remote connectivity to the corporate network became a reality and employees were now able to gain access to company information via different devices, such as mobile phones and notebook computers, using a data-enabled communications network.

As a result, these advances in technology made it much easier and faster to obtain the required information, but these advances also introduced new risks in terms of the security of organisational information. Access restrictions across a multitude of connectivity mechanisms, securing data on mobile devices are but a few examples of issues which were introduced. It has become clear that the majority of organisational information was being stored and processed on the organisational IT infrastructure and spread across data centres, networks, servers and different applications and databases.

Since good corporate governance has become a critical requirement for any organisation, any issue which can contribute towards the overall well-being of the organisation, whether constructive or destructive, should be seen as important and critical to good corporate governance. Information and the IT infrastructure it relies on are very important to the organisation. Therefore, the governance of information and its related technologies should be seen as a corporate governance issue (IT Governance Institute, 2007). Implementing a properly-governed and efficient IT infrastructure is therefore a big contributor to sound corporate governance within an organisation.

An organisation's risk of failure due to bad governance is reduced if it has an effective IT infrastructure and systems which are always available, secure and deliver the correct information to the correct entity at the correct time and in the correct format. Having such an effective infrastructure will not only minimize business-related risks, but also enhance the performance of the business processes. For this reason, it is important to discuss IT governance in more detail.

2.4 IT Governance

IT governance can be defined as "a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes (IT Governance Institute, 2000a)." Advances in IT have made various solutions and applications available to a multitude of business requirements. However, these new technologies and applications also introduced many new risks and although many companies gain value by implementing new technologies, successful companies also manage the risks which are associated with them (IT Governance Institute, 2000a).

The IT Governance Institute (2007b) published the "Control Objectives for Information and related Technologies" (COBIT) framework which guides organisations towards sound IT governance. COBIT is a very popular framework and is recognised in over 100 countries. It is currently in its fourth edition and continues to be refined and amended as technology advances (IT Governance Institute, 2007b).

According to IBM, many of its clients focus on IT governance for the following two reasons: firstly, in order to meet and document compliance to certain external business practices, such as Sarbanes-Oxley and Health Insurance Portability and Accountability Act (HIPPA) and secondly, for the desire to deliver more value to the business from its IT operations and investments (Cantor & Sanders, 2007).

With the many benefits that IT holds for organisations today and the many systems which form part of its information network, it can be concluded that IT is not merely a "nice-to-have" investment anymore for any organisation, but rather an important foundation on which to base its business processes. If an organisation is to survive and be success, it is critically important that its information and IT systems be properly governed.

2.4.1 The Relationship between IT Governance and Corporate Governance

IT governance aims to support corporate governance by protecting the information assets and aligning the strategy of the IT infrastructure with business processes in order to effectively and efficiently strive towards meeting the organisational objectives. It also ensures that any further developments and new applications will be properly aligned.

It should ultimately be the Board of Directors' (BoD) responsibility to understand the risks and benefits of implementing IT, since most business procedures and operations rely mainly or entirely on IT. Therefore, it should also be the BoD who should be responsible to ensure that the IT infrastructure of the organisation is properly governed (McCue, 2007).

IT and specifically IT security were always considered a technical issue by the board and therefore the responsibility for IT governance were delegated to the IT department in the organisation. This is definitely no longer the case. IT governance and corporate governance can therefore no longer be seen as two separate disciplines, with the responsible entity for implementing IT governance lower down in the organisational hierarchy (Gamma, 2007). Figure 2.1 depicts how IT governance is related to corporate governance, with risk management being a core objective of IT governance.

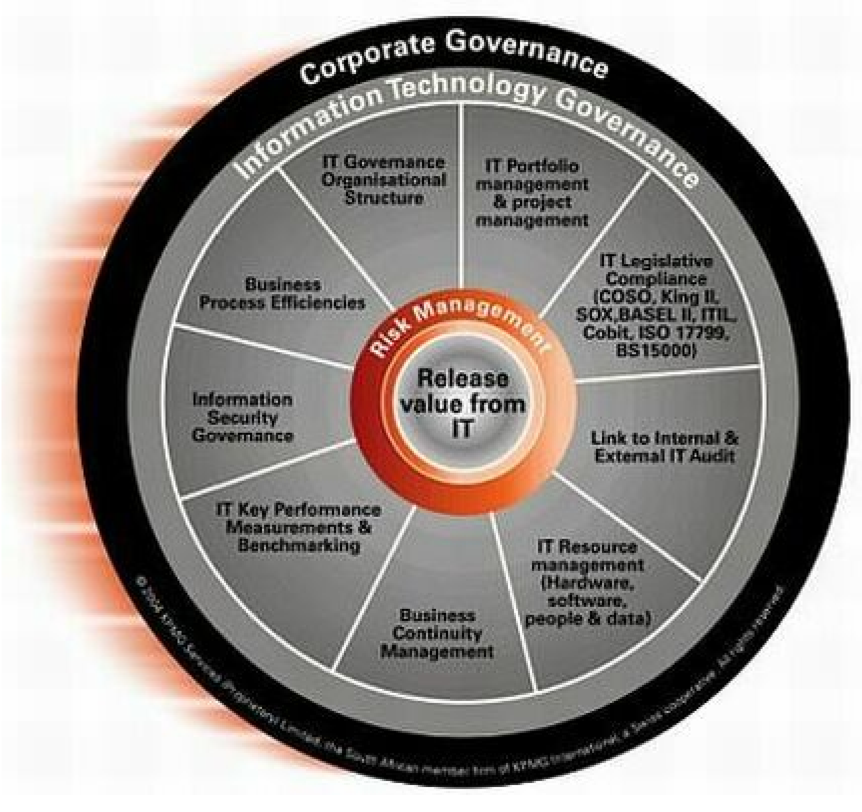

Corporate Governance
Information Technology Governance
IT Governance Organisational Structure
IT Portfolio management & project management
IT Legislative Compliance (COSO, King II, SOX,BASEL II, ITIL, Cobit, ISO 17799, BS15000)
Link to Internal & External IT Audit
IT Resource management (Hardware, software, people & data)
Business Continuity Management
IT Key Performance Measurements & Benchmarking
Information Security Governance
Business Process Efficiencies
Risk Management
Release value from IT
© 2004 KPMG Services (Proprietary) Limited, the South African member firm of KPMG International, a Swiss cooperative. All rights reserved.

Figure 2.1: Corporate and Information Technology Governance (KPMG, 2004)

2.4.2 Objectives of Information Technology Governance

Information technology governance's primary goals are: firstly, to understand the issues and the strategic importance of IT, to ensure that the organisation can sustain its business operations and processes and to ensure that it can implement the strategies required to expand its operations in the future (IT Governance Institute, 2000a). It deals with more than only managing the IT infrastructure which is currently in place.

There are many applications and technologies available today which can provide value to an organisation. It is, however, important to strategically decide which of these is needed to support that organisation. It can be seen that an application of technology can work well on its own, but if it does not support the objectives and direction of the organisation, then it is not supportive, but rather valueless.

It is, therefore, important to invest in an IT application which suits the requirements of the organisational objectives, i.e., supportive of the objectives. It makes no sense to have an IT investment which works well, but it does not support the objectives of the organisation. After all, technology should not dictate how to do business; it should support, enhance and provide value to current business processes.

Ludo Vandervelden, Vice-President of Toyota Motor Marketing Europe, stated that his company's efforts towards good IT governance paid off, resulting in enhanced operations, providing tools for cost and control, reducing adverse budget impacts and helping to make all parties more accountable (KPMG, 2004). This is one of many success stories about the benefits of good IT governance.

2.4.3 Governance Best Practices in South Africa

Corporate and IT governance implementation efforts may require substantial efforts and resources. To provide direction towards implementing IT and corporate governance, various legislative and compliance guidelines and practices have been published. The King II report of 2002 addresses good corporate governance and provides in-depth guidance regarding the BoD's responsibilities (King Report, 2002). The King report was originally published in 1994 by the King Committee on Corporate Governance as King I (Cliffe Dekker, 2002). The evolving global economic environment and legislative developments necessitated that this report be updated. The updated report was published in 2002 as the King II report. Its main objective is to "promote the highest standards of corporate governance in South Africa" (King Report, 2002) and is a very prominent source for information on corporate governance in South Africa. Although the King and King II reports contains guidelines and stipulates what is expected of good governance, they do not demand compliance, since they are not legislative acts (Thompson, 2003).

There are various other international standards, best practices, publications and regulations in existence which provide information and guidelines in order to implement good IT governance within an organisation. COBIT (IT Governance Institute, 2007b) was introduced earlier in the chapter and is explored in greater detail in chapter 3. The ISO 17799 code of practice for information security management also exists. This standard defines internal controls and procedures to protect the organisation's information assets (Standards South Africa, 2005b).

2.4.4 Implementing IT governance

In order to be successful, a structured approach needs to be followed when implementing IT governance in an organisation. The driving force should be the top-level management which should drive the implementation with a top-down approach. A board has to recognize its responsibility to encourage and oversee implementation of good IT governance processes and procedures in its organisation (IT Governance Institute, 2007a).

COBIT provides the organisation with 34 high-level objectives, covering more than 300 detailed control objectives (IT Governance Institute, 2007b, Page 62). The objectives provide mechanisms to allow for strategic IT planning, Information Security, Business Continuity, Regulatory compliance, Procurement, Policies etc. Each of these 34 objectives can be implemented and measured according to the COBIT maturity model, a scale of six possible levels of compliance ranging from non-existent to optimised (IT Governance Institute, 2007b, Pages 49-50).

It is not always possible to implement controls and preventative measures in any IT infrastructure to cater for all the applicable risks, since this may incur a lot of cost which may not be justifiable to the value of the specific IT asset (KPMG, 2004). Therefore it is required to determine which threats are most relevant to the IT infrastructure of the organisation in order to plan for the mitigating measures. Thus, the key to successful IT governance is to achieve the appropriate balance between risk, value and cost (KPMG, 2004).

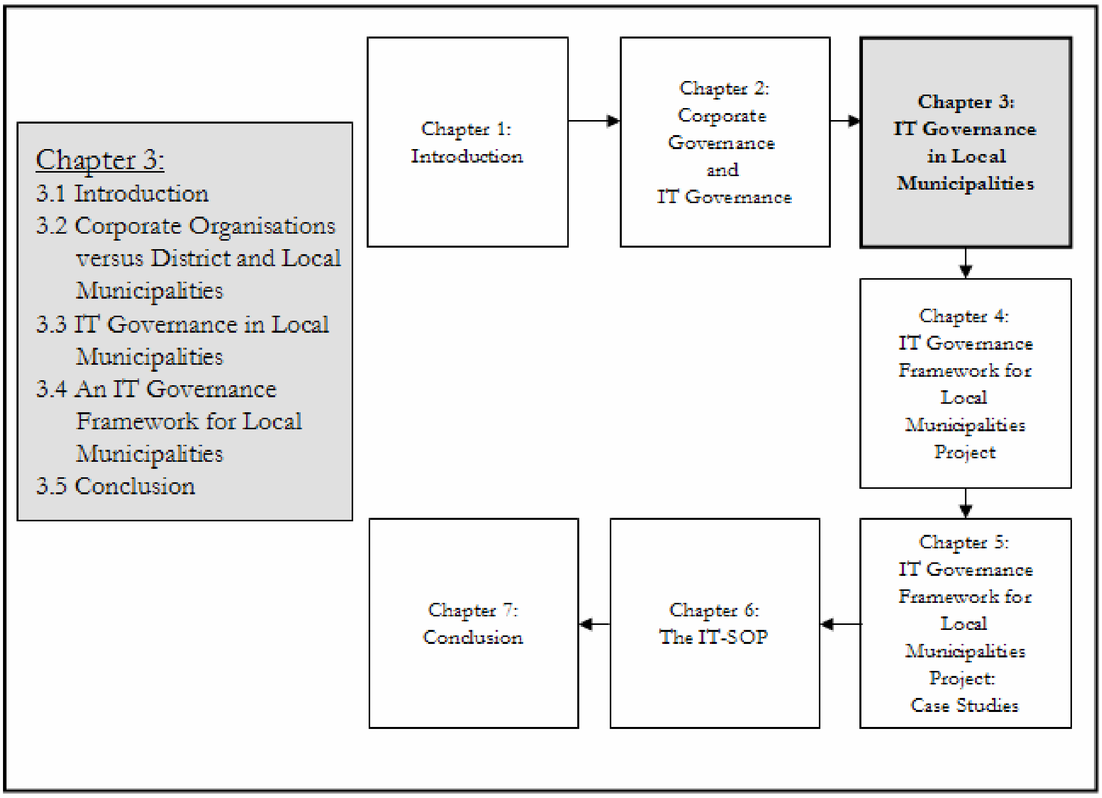
2.5 Conclusion

Corporate governance and IT governance are no longer separate, independent processes, but rather a single, integrated process to better govern an organisation. Investors regard good corporate governance as a hallmark of quality and would be willing to pay more for shares of a well governed organisation. Thus, good corporate governance has become a competitive necessity for organisations. As indicated previously, many organisational failures are the result of poor corporate governance. In order for an organisation to be properly governed, it requires accurate information on which to base its business decisions. Information is an organisation's most valuable asset and therefore it requires the highest level of care and protection in order to maintain its integrity. Since most of an organisation's information are stored and processed by its IT systems, these systems and the governance of the IT infrastructure should be considered a corporate governance responsibility. Therefore, IT is no longer only a technical issue and has become the board's responsibility to ensure that its IT infrastructure is properly governed. There are various standards and practices, such as COBIT and ISO17799 to facilitate the governance of the organisational IT infrastructure.

To further facilitate the understanding of the management of information and the IT infrastructure in South African municipalities, an in-depth analysis of the current state of IT governance in municipalities is discussed in Chapter 3.

Chapter 3

IT Governance in Local Municipalities


Chapter 3:
3.1 Introduction
3.2 Corporate Organisations versus District and Local Municipalities
3.3 IT Governance in Local Municipalities
3.4 An IT Governance Framework for Local Municipalities
3.5 Conclusion
Chapter 1: Introduction
Chapter 2: Corporate Governance and IT Governance
Chapter 3: IT Governance in Local Municipalities
Chapter 4: IT Governance Framework for Local Municipalities Project
Chapter 5: IT Governance Framework for Local Municipalities Project: Case Studies
Chapter 6: The IT-SOP
Chapter 7: Conclusion

3.1 Introduction

As stated in Chapter 2, Information Technology should preferably not dictate the way an organisation should be run or limit its abilities, but rather support and complement the business processes already in place in order to pursue the objectives of the organisation in a more effective and efficient manner. It makes little sense to invest huge amounts of money into IT systems which have little value to the organisation. The systems may function properly on their own, but if they do not add value (perform more tasks in less time, save money, requires less resources etc.) to the organisation, the IT investment can be considered less valuable.

The previous chapter discussed the concepts of corporate governance and IT governance within a corporate (business) environment. The objective of this chapter is to narrow down the scope of corporate and IT governance to focus specifically on how these are implemented in district and local municipalities in South Africa. Firstly, a basic comparison between a municipality and corporate organisation is made in order to understand why IT governance is applicable to both environments. Secondly, the current state of IT governance in municipalities will be explored to understand the lack of good IT governance, as well as various limiting factors. A concept of and the requirements for a good IT governance framework for municipalities will then be proposed.

3.2 Corporate Organisations versus District and Local Municipalities

At first impression, the business goals between these two environments may be very different in nature. For example, a business aims to increase revenue, whereas a municipality aims to use allocated funds to provide services to its constituency. However, there is a multitude of similar business processes found within large corporate organisations, as well as in local municipalities regarding financial administration, human resource management, etc. For instance, the South African Constitution (South African Government Information, 1996) states that "a municipality must structure and manage its administration, budgeting and planning processes to give priority to the basic needs of the community…" Thus, even though both organisations and municipalities may pursue very different objectives, the administrative processes are fairly similar. Therefore, IT governance is essential to municipalities and corporate organisations:

- Both rely on accurate information in order to make strategic decisions;

- Both use IT infrastructures to store, process and utilize data;
- Both rely on employees for data input and output;
- The same threats and risks apply to both corporate and municipal IT infrastructures;
- Both have corporate hierarchies which require various reporting channels and the flow of information;
- Both would benefit if their IT infrastructures were strategically aligned to their business objectives (IT Governance Institute, 2007b, Page 11).

Thus, it is clear that sound IT governance is as important to municipalities as it is to corporate organisations. The current state of IT governance in South African municipalities will now be discussed in the following section to gain broader understanding of the factors which currently limit their governance.

3.3 IT Governance in Local Municipalities

Effective IT governance helps to ensure that IT supports the organisational goals and to appropriately manage IT-related risks and opportunities (IT Governance Institute, 2000a). Failure to properly govern the IT infrastructure of a municipality drastically increases the risk of an unwanted event which may severely cripple the municipality, and not only its IT systems (IT Governance Institute, 2007b, Page 8). Currently, there are various reasons why the IT infrastructures of municipalities in South Africa are not governed to their fullest potential.

A report released in March 2005 by ForgeAhead, a South African research company which specializes in IT development within government, published the results of research in which 284 South African municipalities participated. This report highlighted several severe symptoms resulting from poor, or in some cases, no governance of their respective municipal IT infrastructures (Mochiko, 2005a).

This report stated that municipalities are required, by law, to develop a Master Systems Plan (MSP) in which they describe their current IT infrastructure, as well as envisaged IT projects in order to either maintain or expand the existing infrastructure. However, the report stated the following:

"None of the municipalities in the Northern Cape had an MSP in place for IT

> infrastructure. 90% of municipalities in the Eastern Cape and 80% in Gauteng, Limpopo, the Western Cape and Mpumalanga lacked such a system. About 60% did not know the government policy on IT. Over 90% of municipalities in KwaZulu-Natal and the Northern Cape, and about 70% in Limpopo said they did not understand the policies" (Mochiko, 2005a).

The report stated further that local governments lack proper funding procedures for this implementation, have a shortage of IT skills and do not know the IT sector and its policies.

From the above mentioned statements it can be deduced that South African municipalities are still struggling to implement a sound IT infrastructure that will enhance service delivery for customers and described the symptoms of poor IT governance as arguably the symptoms of a bigger problem: the lack of proper guidelines and legislation which should enable a municipality to be able to implement better IT governance. It is not so much that municipalities have poor IT governance; it is that, in many cases, they have none at all.

Adrian Schofield, head of research at ForgeAhead, made the following statements regarding the results on another study (Mochiko, 2005b) in which 205 municipalities participated in September 2005:

> "The necessity for senior management to invest in infrastructure at a local government level is imperative for effective and sustainable implementation of information and communication technologies". He also stated that although there is an element of IT projects that has been budgeted for and rolled out, this has been left to collapse, creating a sense that IT projects are ineffectual and costly mistakes. This has left an impression with the management that money is better spent elsewhere.
>
> "Though 49% of the Northern Cape municipalities have budgeted for the technology service, the province still lacks the understanding of how to implement those services and products. A concerted effort is needed to find solutions and strategies that will help pull the province out of the current IT slump" the report stated.

At the COGITRIS conference in August 2007 in Port Elizabeth, South Africa, Mr

Heinrich Schnautz, the Data Official in charge of IT at the Oudtshoorn Municipality presented the following table which depicts the status of IT governance in the Eden district in the Southern Cape region:

Table 3.1: IT Structures and Staff in the Eden District

Municipality	**Reporting Structure of the IT Manager**	**IT Staff**	**Data Operators**	**Total Staff**	**Total Personnel**	**Total Users / PC's**	**Ratio**
Eden	Acting Director – Internal Planning	5	N/A	7	700	280	1 / 56
Bitou	Municipal Manager	3	N/A	3	200	160	1 / 53
George	Asst Dir Finance	2	N/A	2	850	450	1 / 225
Hessequa	Municipal Manager	2	N/A	2	480	125	1 / 75
Kannaland	Director Finance	0	N/A	0	98	25	-
Knysna	Director Finance	6	N/A	6	630	260	1 / 43
Mossel Bay	Director Finance	2	N/A	2	766	250	1 / 125
Oudtshoorn	Asst Dir Finance	1	N/A	1	645	120	1 / 120

The following conclusions can be drawn from the above table:

- There are various different reporting lines for IT managers. Although two out of the eight municipalities report directly to the municipal manager, there is still no council-level representation of the IT function.

- There exists a very high ratio between municipal IT users and the employees within the IT function of a municipality.
- The high ratio between employees and IT employees does not only overburden current IT staff with everyday IT support issues, preventing them from performing strategic planning and development for the IT function, but it also introduces various risks. Having so few IT employees practically eliminates duty segregation as well as poses a serious continuity threat, should a key IT employee (or in some cases, the only IT employee) be relieved from his/her duties from the municipality, whether through resignation or retrenchment.

There are various other examples of poor IT governance within municipalities. They serve as an indication as to how little recognition is given to the importance of information and IT.

Adrian Schofield (Mochiko, 2005b) states that many IT projects from municipalities fail, leaving the impression that the money is "better spent elsewhere." For this reason, Schofield claims that municipalities have become reluctant to invest effort and strategy into acquiring a sound IT infrastructure and good IT governance processes, possibly because of the lack of proper standards or guidelines regarding IT development in government. As a result, municipalities have each invented their own IT 'wheel', consisting of their self-sourced hardware, software and basic management procedures thereof. These are very often based on and built-up from internal knowledge of employees, instead of from well-known procedures and principles, such as best practices. Thus, many municipalities now have their own information 'islands', accessible only by themselves. Thus, it is now very difficult to exchange skills between municipalities and consolidating and reporting on different information sources within a region is extremely difficult and complex. In the world of commerce, it would not make sense to have different branches of a company each using different point-of-sale, accounting and inventory systems from the other branches. This would severely limit head-office's ability to accurately report on sales figures, inventory levels, etc. The same principle applies to district and the local municipalities related to them.

It is clear that a practical, standard or guideline is needed which can facilitate a municipality to execute proper strategic planning, procurement, development, reporting and maintenance for the IT infrastructure not only for itself, but for the region as a whole.

3.4 An IT Governance Framework for Local Municipalities

There are three fundamental requirements which should be met in order for the proposed IT framework to be successful in municipalities. These are: firstly, it should fit in between the municipal Integrated Development Plan (IDP) and the MSP. Secondly, it should preferably be based on best practices. Thirdly, it should facilitate intergovernmental collaboration regarding various IT issues, such as exchanging of skills, regional strategic planning and IT infrastructure development and maintenance, etc.

3.4.1 Municipal IDP and MSP planning

IDP and MSP planning serve the same purpose for a municipality as business planning serves for corporate organisations. The IDP covers the broad spectrum of municipal planning, whereas the MSP is aimed specifically towards IT infrastructure development.

A corporate organisation, typically, creates long-range strategic plans which state various objectives and growth targets for the next 5 to 10 years, for example. These are often used as bait to lure potential investors. These long-range plans are then translated into short-range plans, stating various milestones and short-term objectives which are overall supportive of the overall, long-range objectives. In essence, the long-range plans describe the vision and what needs to be achieved, whereas the short-range plans describe how the objectives will be met, as well as in more detail (Compass Point, 2006).

The same principles apply to the municipal IDP and MSP plans. The IDP deals with the broad vision and strategy of community service delivery (Government Gazette, 2000) and the MSP deals specifically with the IT infrastructure and systems of the municipality. The key issue is to ensure that the MSP contents, strategies and objectives reflect the needs of the IDP. In other words, the MSP should be strategically aligned with the objectives of the IDP.

Therefore, it is critical that appropriate management processes and procedures are in place which will ensure that the IDP is properly translated into the MSP. Without it, the MSP runs the risk of being not aligned with the IDP. This will result in the municipal objectives and the IT objectives being steered in different directions.

The following figure depicts where the proposed framework will fit in between the IDP and the MSP of a municipality:

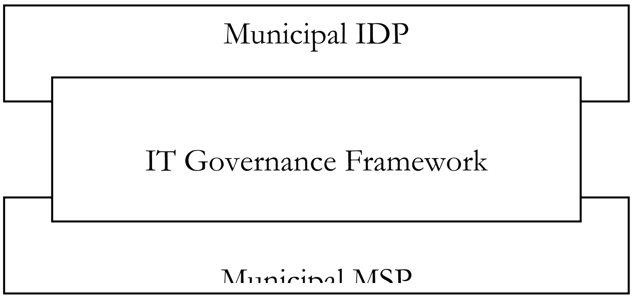


Figure 3.1: Positioning of the IT Governance Framework

3.4.2 Best Practices and Standards

For any organisation, such as a local government, to be well governed, it must incorporate and base its operating strategy on best practices (IT Governance Institute, 2000b). Best practices can be defined as the most efficient (least amount of effort) and effective (best results) way of accomplishing a task, based on repeatable procedures that have proven themselves over time for large numbers of people (Wu, 2007). It can, therefore, be said that it is streamlined procedures which have been developed and refined by people and organisations for a certain span in time. It ensures that the desired outcome is met as best as possible, while requiring as few resources (time, money, human, tangible) as possible.

There are various international best practices, standards and guidelines which focus on or support effective IT governance. The Control Objectives for Information and related Technology (COBIT), the International Organisation for Standardisation (ISO) 17799 for Information Security and the Information Technology Infrastructure Library (ITIL) are examples of these. COBIT and ISO 17799 were used extensively and is core to the proposed IT governance framework. In order to gain better understanding of what COBIT and ISO 17799 entails, they will both be discussed in more detail.

3.4.2.1 Control Objectives for Information and related Technologies (COBIT)

COBIT is a guideline for management objectives and processes for IT governance within organisations and is published by the Information Systems Audit and Control Association (ISACA). It is currently in its 4th edition, but is continually updated and expanded. It is recognized and used in more than 100 countries as a solid foundation on which to base IT management processes (IT Governance Institute, 2000b). COBIT was chosen for this project for two reasons: firstly, municipalities' IT systems are audited on an annual basis against COBIT by the office of the Auditor General and secondly, "COBIT is, in many cases, preferred by IT auditors and IT risk managers as a framework of choice", according to von Solms (2005). Therefore, a framework can be proposed which is based on the same requirements as the auditors' measurement metrics and requirements. The COBIT framework will now be discussed in more detail.

COBIT consists of 34 high-level objectives, which are grouped into four domains. These are: Plan and Organise (PO), Acquire and Implement (AI), Deliver and Support (DS) and Monitor (M). Each of the 34 high-level objectives is made up of numerous detail processes which can be performed. These high-level objectives cover a total of 314 detail processes (IT Governance Institute, 2000b).

At the time of conducting the research, COBIT was in its 3rd edition. Therefore, the structure of the 3rd edition is discussed from here onwards. The following table depicts the four COBIT domains, with their respective objectives, in order to gain better understanding of COBIT.

Table 3.2: COBIT 3 High-level Control Objectives

Objective Prefix	**Objective Name**
Domain: Plan and Organise	
PO1	Define a strategic IT plan
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Organisation
PO5	Manage the IT Investment
PO6	Communicate Management Aims and Direction
PO7	Manage IT Human Resources
PO8	Ensure Compliance with External Requirements

PO9	Assess and Manage IT Risks
PO10	Manage Projects
PO11	Manage Quality
Domain: Acquire and Implement	
AI1	Identify Automated Solutions
AI2	Acquire and Maintain Application Software
AI3	Acquire and Maintain Technology Infrastructure
AI4	Develop and Maintain Procedures
AI5	Install and Accredit Systems
AI6	Manage Changes
Domain: Deliver and Support	
DS1	Define and Manage service levels
DS2	Manage third-party services
DS3	Manage performance and quality
DS4	Ensure continuous service
DS5	Ensure systems security
DS6	Identify and Allocate costs
DS7	Educate and Train users
DS8	Assist and advise customers
DS9	Manage the configuration
DS10	Manage problems and incidents
DS11	Manage Data
DS12	Manage Facilities
DS13	Manage Operations
Domain: Monitor	
M1	Monitor IT Processes
M2	Assess Internal control adequacy
M3	Obtain independent assurance
M4	Provide for independent audit

COBIT also provides a maturity model which can be used for measuring the current level of management for each of the high-level objectives. This model consists of six possible levels which are:

- **Non Existent:** Complete lack of any recognizable process. The organization has not even recognized that there is an issue to be addressed.
- **Initial/Ad Hoc:** The organization has recognized the issue exists and needs to be addressed. Ad-hoc approaches, instead of standardized processes, are applied on an individual or case-by-case basis. The overall approach to management is disorganized.
- **Repeatable:** The process has been developed to a stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and therefore, errors are likely.
- **Defined Process:** There are standard and documented procedures. These have been communicated through training. It is, however, left to the individual to follow these processes, and is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalization of existing practices.
- **Managed and Measurable:** It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
- **Optimised:** Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modeling with other organizations. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness so making the enterprise fast and adaptable (IT Governance Institute, 2000b).

Each maturity level has its own tradeoffs. The higher maturity level the organisation wishes to achieve for any given process, the more resources, time and commitment will be required, but it will result in a better-managed process. For all 34 high-level objectives, it is not always required to implement all of them at a maturity level 5, since some objectives are less applicable to the nature of the organisation. It is also important that one should not, as mentioned in the previous chapter, invest more resources in the protection and management of an asset than what it is worth and its value to the organisation. The key is to find a balance between cost, effectiveness and risk (KPMG, 2004). The risk which remain after mitigation strategies have been implemented, are called the residual risk (Allen, 2006). This remaining risk is often formally accepted by organisations and preventative actions for this risk are usually taken in the form of third-party insurance. Thus, it is acceptable to determine a maturity level which suits the organisational nature regarding risk, cost and the effectiveness of the mitigation strategies for IT management processes.

Information security is also a very core aspect of IT governance. COBIT has its own high-level objective, DS5, which deals with information security: "Ensure systems security." There are also, apart from DS5, many other detailed processes within the other 33 high-level objectives which also fall within the information security domain. These processes are described in little detail, but they explain what should be done for the process to be successful. This high level, abstractive description leaves room for interpretation. To ensure that municipalities implement proper and adequate security measures, the ISO 17799 standard, which deals with information security, states very clearly and in great detail exactly how to implement various security controls. Therefore, the ISO 17799 standard will now be discussed, as well as reasons why COBIT and ISO 17799 complement each other very well and can be implemented simultaneously.

3.4.2.2 ISO 17799 Code of Practice for Information Security Management

The ISO 17799 standard deals with information security within an organisation. Since July 2007, this standard has been renumbered to the ISO/IEC 27002 standard. For the purposes of this dissertation, and because the conducted research was done under the 17799 numbering, the remainder of this dissertation will refer to the standard as ISO 17799.

The standard consists of 11 main security control clauses, covering a total of 39 main security categories. The main security control clauses are (Standards South Africa, 2005b):

a) Security Policy
b) Organizing Information Security
c) Asset Management
d) Human Resources Security
e) Physical and Environmental Security
f) Communications and Operations Management

g) Access Control
h) Information Systems Acquisition, Development and Maintenance
i) Information Security Incident Management
j) Business Continuity Management
k) Compliance.

It is not necessary to implement all of the controls as specified in the standard for the following two reasons: Firstly, an organisation is expected to conduct a structured information security risk assessment process in order to determine the specific requirements before selecting controls which are appropriate to its nature. Secondly, it is practically impossible to list all of the conceivable controls in a general purpose standard. Each industry has specific requirements which can be drawn from this standard (Standards South Africa, 2005a). There are, however, three essential controls and seven common-practice controls for information security. The essential controls are: data protection and privacy of personal information, protection of organisational records and protection of intellectual property rights. The common practice controls are: an information security policy document, allocation of information security responsibilities, information security awareness, education and training, correct application processing, technical vulnerability management, business continuity management and the management of information security incidents and improvements. These controls apply to most organisations in most circumstances (Standards South Africa, 2005a). The standard states that although all of the controls are important and should be considered, the relevance of any control should be determined in the light of the specific risks which an organisation is facing.

Even though the ISO 17799 standard and COBIT contain information security processes, there are various processes and controls that complement each other. For this reason, ISACA published a document which maps the ISO security clauses and controls to their respective COBIT objectives and processes. There are numerous reasons why COBIT and ISO 17799 can be implemented together (von Solms, 2005). These are:

- ISO 17799 is more detailed than COBIT; therefore, it provides guidance on exactly how things should be implemented, whereas COBIT provides a much broader, less detailed description, focusing more on what needs to be done.

- ISO 17799 provides very much 'stand-alone' guidance and does not provide the broad IT governance spectrum like COBIT does. Therefore, it is recommended to use ISO 17799 in conjunction with COBIT.

Von Solms (2005) also states that: "It therefore seems logical that to get the benefits of both the wider reference and integrated platform provided by COBIT, and the more detailed guidelines provided by ISO 17799, there can be a lot of benefit in using both together for Information Security Governance. The synergy of combining these two frameworks can be substantial. To a certain extent, these two frameworks naturally complement each other."

Developing an IT governance framework for municipalities, which is based on the COBIT and ISO 17799 frameworks, would ensure that internationally recognised best practices and procedures are employed in order to successfully manage a municipal IT infrastructure. Within a district municipality and its underlying local municipalities, this proposed framework holds plenty of advantages if it is implemented within the region as a whole. Therefore, it is suggested that the municipalities proactively engage in a joint, strategic collaboration effort in order to successfully implement such a framework.

District and local municipalities are able to provide support services to one another upon request, as described in the Municipal Structures Act, No. 117 of 1998 (Government Gazette, 1998). In order to understand these intergovernmental relationships and how they can facilitate in this framework implementation, it is necessary to briefly discuss the types of municipalities, as well as how they can interact with one another in the light of providing services.

3.4.3 Municipal Intergovernmental IT Collaboration Framework

The Municipal Structures Act, No. 117 of 1998, specifies three types of municipalities which can be established within South Africa. An "A"-type municipality is considered a metropolitan municipality. This type is responsible for providing service to the whole region. For a region which does not constitute a metropolitan area, a district- ("B"-type) and underlying local municipalities ("C"-type) should be established. According to the Municipal Systems Act, No. 32 of 2000, a C-type municipality should provide the same services as B-type municipalities, as well as provide coordination between itself and its underlying B-type municipalities (Government Gazette, 2000).

The Municipal Structures Act prescribes three ways in which municipalities can provide support services to another municipality within the same region. The act describes these as general support services, but they can apply to IT support services as well. These three support services scenarios are described as:

1. A C-type municipality may provide support services to a B-type municipality upon request, providing that it has the required capacity in order to provide this service.
2. A B-type municipality may provide support services to a C-type municipality within the region upon request.
3. A B-type municipality may provide support services to another B-type municipality within the region upon request.

The following figure graphically depicts these intergovernmental support-service scenarios:

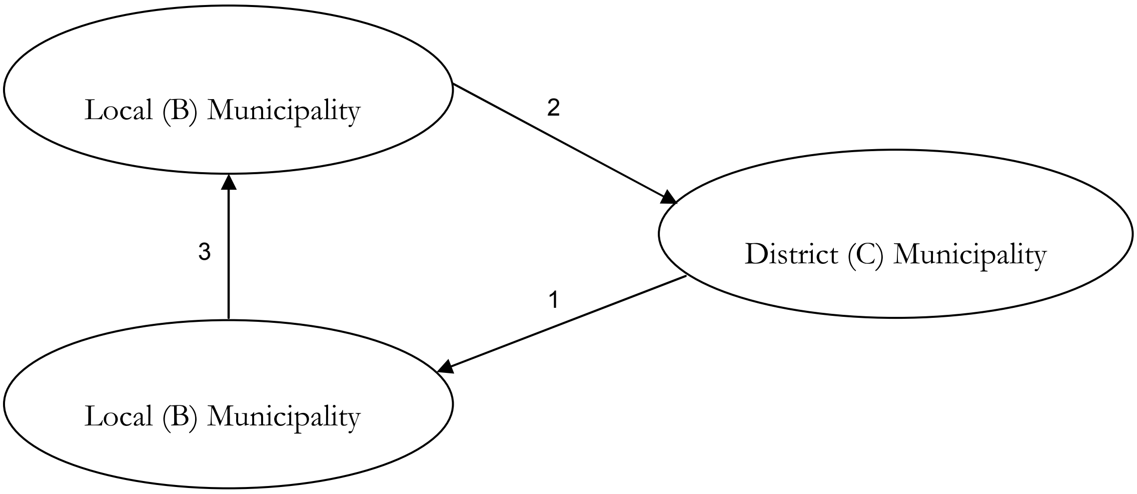


Figure 3.2: Municipal Intergovernmental Support Service Scenarios

In order for a municipality to provide IT support services to another municipality, whether these services are of a strategic, development or maintenance nature, would be much more effective if the IT governance processes are based on the same IT governance framework. Municipalities would, thus, be able to compare "apples with apples", since they would all be familiar with the same IT strategic, development and maintenance governance processes.

3.5 Conclusion

Municipalities' and corporate organisations' missions and objectives are different, but have similar administrative functions. Therefore, Corporate and IT governance are applicable to both corporate organisations and government municipalities. However, municipalities in South Africa are still struggling to implement proper IT infrastructures and sound IT governance. As a result, the many advantages of an efficient and effective IT infrastructure and governance processes are still unutilized. This scenario is further inhibited by the current lack of guidelines and standards for municipalities on which to base their IT implementations on. Municipalities are thus in need of a practical and strategic framework to assist them in implementing an effective and efficient IT infrastructure as well as sound IT governance processes.

To aid municipalities in the development of IT governance procedures, the three basic elements of the proposed IT governance framework were discussed. These three elements are the placement of the framework between the IDP and MSP, the use of best practices and standards as basis for the framework and lastly that the framework should facilitate intergovernmental support for the sharing and collaboration of IT governance.

The COBIT framework and ISO 17799 standard were discussed as well as the roles which they play in IT governance and in this framework and how municipalities can provide support services in the form of IT-strategic, development and maintenance to one another in the region.

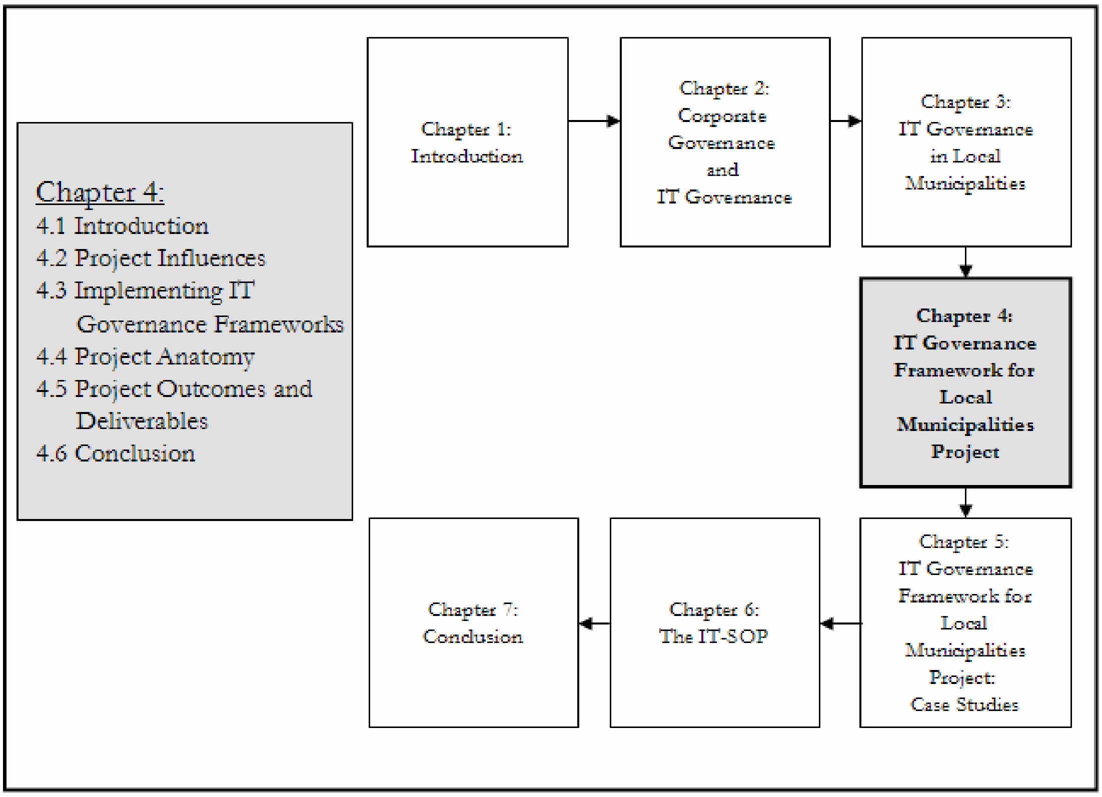
The next chapter focuses on the IT governance framework for municipalities. It discusses the initial project requirements which were needed to be able to propose this framework. The project layout, deliverables and key issues, such as sustainability are then also discussed.

Part III

Solution

Chapter 4

IT Governance Framework for Local Municipalities Project



Chapter 4:
4.1 Introduction
4.2 Project Influences
4.3 Implementing IT Governance Frameworks
4.4 Project Anatomy
4.5 Project Outcomes and Deliverables
4.6 Conclusion
Chapter 1: Introduction
Chapter 2: Corporate Governance and IT Governance
Chapter 3: IT Governance in Local Municipalities
Chapter 4: IT Governance Framework for Local Municipalities Project
Chapter 5: IT Governance Framework for Local Municipalities Project: Case Studies
Chapter 6: The IT-SOP
Chapter 7: Conclusion

4.1 Introduction

The previous chapter discussed the current state of IT governance in local municipalities. It was argued that a framework and guidelines are required for the effective governance of IT within local municipalities. This framework and guidelines should facilitate municipalities to align their IT operations with the municipal objectives and to develop, govern and monitor their IT infrastructure and associated systems.

This chapter discusses the project layout that was conducted at a district municipality and its underlying local municipalities. The factors that influenced the current state of IT governance and the project are briefly summarized and the project anatomy is explained.

4.2 Project Influences

There are various factors that have an influence on the current state of IT governance within local municipalities. The first factor is the municipal legislation, which does not stipulate the requirements for effective IT governance within local municipalities. The second factor is the lack of proper guidelines and standards, which should assist municipalities to develop and govern an IT infrastructure and associated systems that are representative of their requirements. As discussed in Chapter 2, there are many IT governance implementation frameworks, but these provide a holistic view of IT governance in general and not tailored to suit any specific environment. This lack of guidelines and standards has resulted in municipalities implementing their own, proprietary IT infrastructures with few associated governance processes. This has, in turn, caused a third factor, the lack of coordination and synchronization between municipalities, specifically their IT systems. Many municipalities now operate on different financial, spatial and human resource systems.

The municipal IDP is the fourth influential factor, since this plan describes the municipal objectives for the following five to 10 years. This plan is similar to an organisation's long-term strategic plan. The IT governance processes and infrastructure that result from the implementation of the framework should be reflective of the objectives and requirements as set out in the IDP. The fifth factor is the MSP. This is the detailed plan that describes the IT infrastructure and the governance thereof. It is of critical importance that the MSP plan is aligned with the IDP in order for the MSP to reflect the requirements of the IDP, but is translated into IT systems' requirements and governance processes. Therefore, the IT governance framework should be placed between the IDP and MSP, in order for the MSP to be properly aligned with the IDP. This framework placement was discussed in the previous chapter. The MSP is also dependent on the sixth and last factor, the annual IT audit report.

Municipalities' IT systems are audited on an annual basis to determine whether the internal controls are satisfactory before the financial information is audited (George Municipality, 2006). This audit is conducted by the office of the auditor general and the municipality is audited against COBIT. It is important that the risks (shortcomings) identified during the audit process be incorporated into the MSP to ensure that these risks are mitigated. COBIT was, therefore, chosen as the IT governance framework of choice, since using it for this project will also ensure that the audit requirements are met, since COBIT, as stated in the previous chapter, is widely recognized as an IT governance framework. These six factors all influence the current IT governance problem in local municipalities. The audit reports of the district municipality and those of the underlying local municipalities indicate that there is a significant lack of proper IT governance procedures and internal controls. A solution is an IT governance framework tailored for the requirements of local municipalities. This framework should be able to be implemented within the municipalities of a district. It should facilitate these local municipalities to develop acceptable processes, procedures and internal controls. These can then possibly be communicated to other municipalities within the region or even wider. Some of the results of the successful implementation of this framework could be joint strategic planning between regional municipalities, compatible systems and accurate, valuable information.

Figure 4.1 depicts this IT governance project, factors of influence, the current situation and the proposed solution:

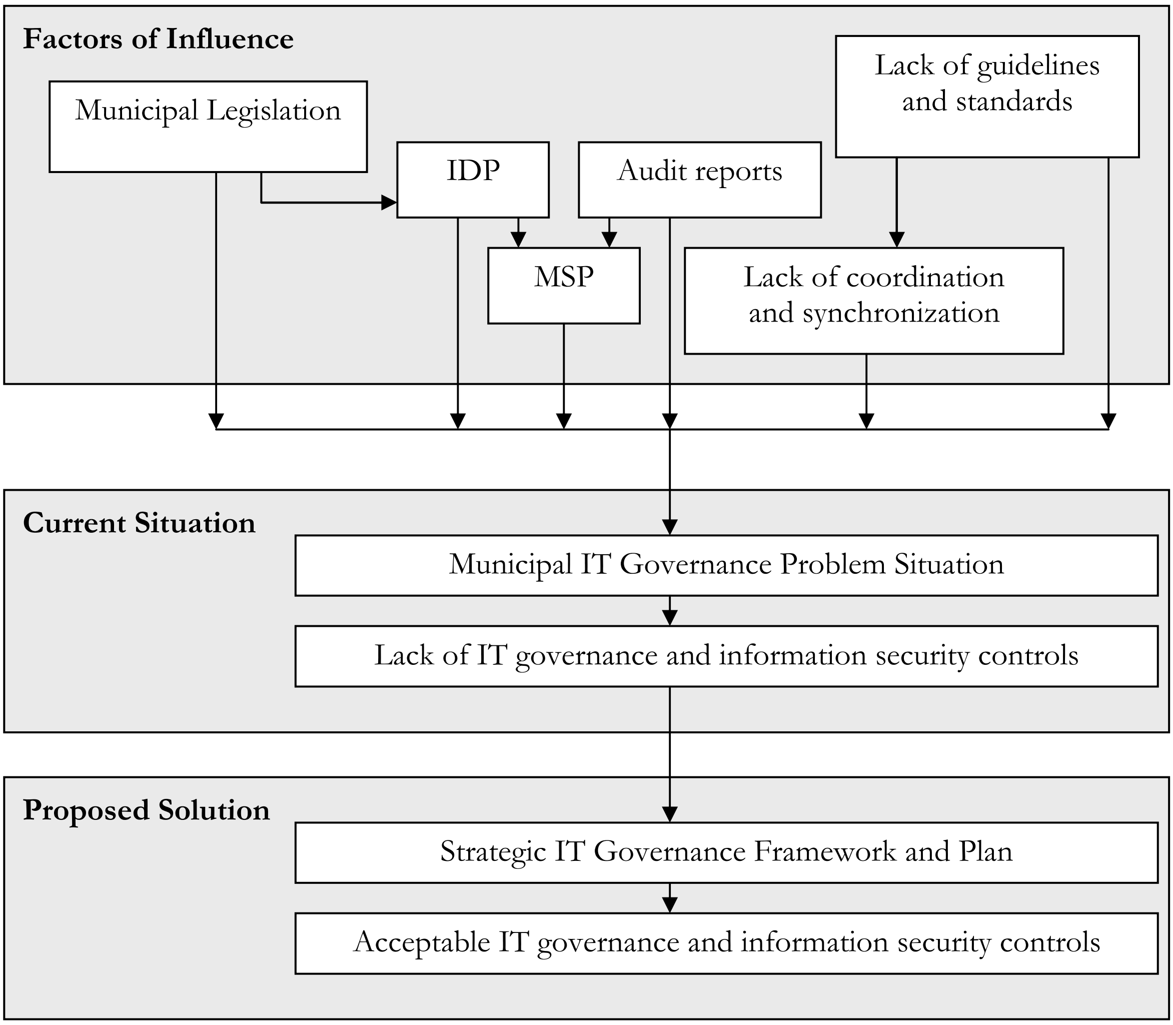

Factors of Influence
Municipal Legislation
IDP
Audit reports
Lack of guidelines and standards
MSP
Lack of coordination and synchronization
Current Situation
Municipal IT Governance Problem Situation
Lack of IT governance and information security controls
Proposed Solution
Strategic IT Governance Framework and Plan
Acceptable IT governance and information security controls

Figure 4.1: The IT Governance Project

From Figure 4.1, it is possible to see how the various factors contribute towards the current IT governance problem situation in local municipalities. This has led to a lack of proper IT governance and information security controls. The proposed solution includes a framework for processes and controls, as well as an implementation plan to facilitate the implementation of the framework. The result of the successful implementation of the plan is acceptable IT governance procedures, processes and information security controls within the local municipality.

In order to understand how governance frameworks are implemented, the framework implementation requirements and the steps involved will now be discussed.

4.3 Implementing IT Governance Frameworks

In Chapter 2, it was argued that corporate and IT governance can no longer be separated. Successful IT governance within a municipality should represent an organisational structure, as well as a set of processes and procedures, which manage and control the municipality's IT activities (Kordel, 2004). This structure should be embedded in the organisation and be applied to all IT activities and processes.

Poole (2007) suggests that implementing IT governance causes cultural change within an organisation. Implementing IT governance, therefore, cannot be considered as only a once-off project. It is, rather, a continuous endeavour, or life cycle (Kordel, 2004), towards an organisation-wide culture of ongoing IT governance activities. Thus, IT governance is considered part of the corporate culture of the municipality.

In order to incorporate an IT governance culture within the municipality, it is necessary to implement an IT governance framework. The framework implementation can be considered as a series of implementation projects (Kordel, 2004). In essence, the smaller implementation projects should form part of an overall implementation strategy, facilitating an organisational culture change towards successful IT governance.

Implementing an IT governance framework requires the development of an effective governance approach (Poole, 2007): first, that it is important to realize the business advantages which is gained from implementation. The municipality should understand what will be gained from the exercise, i.e., why this implementation is taking place. Advantages such as IT responsibility and accountability, IT aligned with business objectives, ensuring return on investment and risk management are all part of these business advantages (Poole, 2007).

The second pre-requisite is obtaining management buy-in. This is of critical importance, since the executive management (municipal council) should take ownership of IT governance and set strategic direction. The council should realize that IT governance is its responsibility and that it forms part of the overall organisational governance (Poole, 2007). According to the CHAOS report (Marchewka, 2003), management buy-in is one of the requirements ranked at the top of the list which is required for successful project implementation.

The third pre-requisite is to establish a project plan. This plan should establish sub-projects, which provide steps for the alignment of the IT strategy with business goals, risk definitions, analyse current capability, gap identification and the development of improvement strategies (Poole, 2007). These three steps are shown in Figure 4.2.

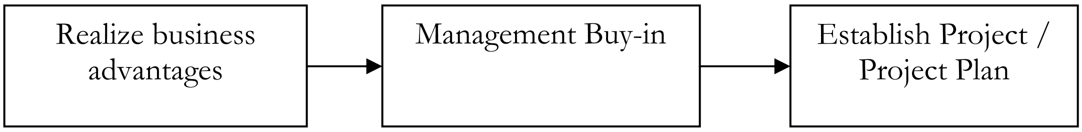


Figure 4.2: Establishment of a Governance Approach

Poole (2004) further suggests that the implementation initiative should be treated as a project activity, with a series of phases, as a proven factor in the successful implementation of an IT governance framework. These phases should be treated as small projects that should be able to be completed within a year (Marchewka, 2003). The reason for this is that large projects only have a success rate of 9% and are much more risky than medium or smaller projects. After establishing the governance approach, it is necessary to develop the steps required for the implementation of the framework as part of the project plan.

The *IT Governance Implementation Guide* (Kordel, 2004) prescribes four steps when implementing an IT governance framework. The first step is to identify the project requirements. In this step, the scope of the improvement project is decided upon. The COBIT Key Goal Indicators (KGIs) and the Critical Success Factors (CSFs) are used to help determine the IT goals. Also, the COBIT control objectives provide information on the processes and controls required for the mitigation of business risks.

The second step is to envision the solution. This step prescribes that the current maturity of the selected IT processes be evaluated (as-is) against the COBIT maturity model. It is also prescribed that the target maturity levels (to-be) should be set. According to this implementation guide, the gaps between the as-is and the to-be levels are then translated into improvement opportunities (Kordel, 2004).

The third step is to plan the solution. This step involves the identification of feasible improvement opportunities and translating them into justifiable projects. After these projects have been approved, they are then incorporated into an overall improvement strategy. These projects are then prioritized, and metrics may be set using COBIT's KGIs and Key Performance Indicators (KPIs).

The fourth step is to implement the solution and its sub projects. The implementation efforts are measured according to COBIT's KGIs and KPIs. After implementation of the IT governance framework, a continuous life-cycle begins where the IT governance processes are measured and monitored and new improvement opportunities identified. These four steps of the IT governance implementation plan are depicted in Figure 4.3.

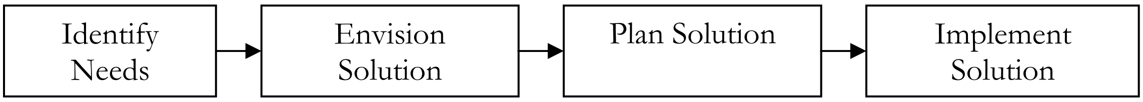


Figure 4.3: IT Governance Implementation Plan

Using the governance approach (Figure 4.2), in conjunction with the IT governance framework implementation plan (Figure 4.3), achieves a combined implementation strategy. Figure 4.4 depicts the combined implementation strategy.

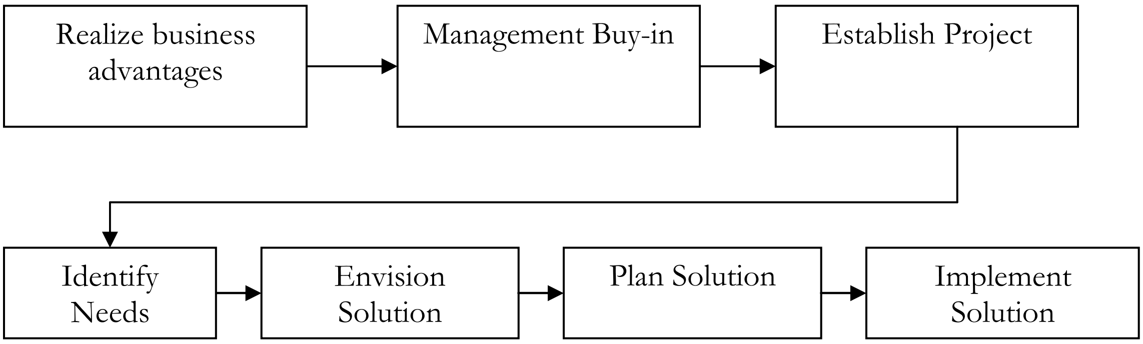


Figure 4.4: Combining the Governance Approach and the IT Governance Implementation Plan

The above-mentioned combined implementation strategy was used to conduct the required live case study at the district municipality and its underlying municipalities. The implementation strategy led to the following identified phases and steps for the IT governance framework project:

- Phase 1 – Realize Business advantages
  - Step 1: Inform and discuss the benefits of implementing effective IT governance within the municipality – Introduce COBIT, ISO 17799 and their associated advantages to IT management of the municipality.
- Phase 2 – Management buy-in
  - Step 2: Obtain management support by introducing the business benefits, as well as best practices regarding effective IT governance to the executive municipal management – Introduce COBIT, ISO 17799 and advantages to the municipal executive management for their buy-in and support.
- Phase 3 – Plan Project
  - Step 3: Identify Project Needs

        - Step 3a: Define the project scope by identifying the relevant COBIT control objectives for municipalities – determine which COBIT objectives are relevant by means of questionnaire and interviews.
    - Step 4: Envisage the solution – using the COBIT maturity models, questionnaire and interviews
        - Step 4a: Determine the current (as-is) maturity levels of the identified COBIT objectives.
        - Step 4b: Determine the minimum acceptable, or target (to-be) maturity levels for the identified COBIT objectives.
        - Step 4c: Determine the gaps between the as-is and to-be maturity levels. These gaps are the improvement opportunities.
    - Step 5: Plan the Solution (Discussed in greater detail in Chapter 6)
        - Step 5a: Translate the improvement opportunities feasible into micro projects.
        - Step 5b: Prioritize the micro projects and identify measurement metrics.
        - Step 5c: Incorporate the micro projects into the greater improvement strategy.
    - Step 6: Implement the Solution (Discussed in greater detail in Chapter 7)
        - Step 6a: Implement the micro projects as part of the greater implementation strategy.
        - Step 6b: After project implementation, the measurement metrics are used to identify further improvement opportunities.

The application of this structure to the IT governance framework project is discussed in the next section.

4.4 Project Anatomy

The main objective of the live case studies, which was conducted at a district municipality and its underlying municipalities, was to develop a tailored framework for IT governance at municipalities, which is based on COBIT and linked to ISO 17799. This objective was then disseminated further into various sub-objectives. The following paragraphs discuss the layout and the flow of the project and its components.

For step 1, the COBIT framework and the ISO17799 standard were introduced to IT management at the district municipality. During a meeting where various municipal role players (including the municipal manager) were present, the municipality demonstrated a need to enhance its IT infrastructure and its IT governance processes and procedures. The business advantages of implementing COBIT and ISO 17799 were then realized by the IT management. These advantages included IT strategic alignment with the IDP, management ownership of IT, sufficient resources for its governance, risk management and district-wide strategic planning for the IT functions of the district and underlying municipalities. Step 2: the COBIT and ISO 17799 frameworks were then introduced to the municipal council and also accepted as recognized best practices for the municipality. The municipal manager indicated appreciation towards the efforts for the enhancement of IT governance within the district municipality, as well as in the underlying local municipalities. These efforts are in conformance with Poole's first two pre-requisites, realizing the business advantages and secondly, obtaining management buy-in. The third pre-requisite, phase 3, was met by the defining of a project plan. The project plan was determined through a meeting with the IT management of the district municipality and all of the underlying municipalities.

The project plan was set out as follows: step 3a (step 1 in the IT governance implementation guide (Kordel, 2004)) states that project requirements should be determined. This step involves the deciding on the IT processes to be implemented. Therefore, case studies were conducted at the district municipality and the local municipalities to gather the relevant COBIT objectives (the needs). The case studies are further investigated in the next chapter.

Step 4 of the project was performed in order to determine the current (as-is) maturity levels, step 4a, of the COBIT objectives, as well as the target (to-be) maturity levels of each of them, step 4b. The gaps (step 4c) between the as-is and to-be maturity levels were then determined and defined as improvement opportunities. The individual results of the case studies were communicated to the respective municipalities. The individual results were then combined and integrated to provide a holistic view of the requirements for IT governance for the district.

The planning of the solution step (step 5) was conducted by translating the improvement opportunities into smaller, micro projects (step 5a), prioritizing these projects (step 5b) and segregating the overall COBIT framework implementation into various phases, as Poole (2004) and Marchewka (2003) suggest. These smaller projects were then incorporated into the overall improvement strategy (Step 5c). This makes the smaller projects more manageable and increases the success rate of the overall implementation strategy. Applicable ISO 17799 controls were then mapped onto identified COBIT objectives. This process is explained in more detail in the next chapter. Step 6, the implementation of the smaller projects, has been the responsibility of the district municipality to drive the implementation efforts of the underlying municipalities. Municipalities should combine their efforts and provide services to one another, as described in the previous chapter.

The structure and flow of this project conforms to Poole's governance approach and the IT governance's framework implementation guide. The implementation of this structure for the IT governance framework produced multiple outputs and deliverables which are discussed in the next section.

4.5 Project Outcomes and Deliverables

The results from the case studies, applied to the project plan, resulted in the following information:

- The COBIT objectives and processes relevant to the municipality;
- The current (as-is) maturity of each of the relevant objectives and their detailed controls objectives;
- The target (to-be) maturity, which were indicated as being an acceptable target maturity level;
- The gaps between the as-is and the to-be maturity levels.

These results were provided in the form of a report to the municipalities for the identification of improvement opportunities. The various municipal results were combined and incorporated into two reports that were provided to the district municipality (the combining of results and the findings are discussed in the next chapter). The first report indicated the current state of IT governance within the district. The second report contained the COBIT objectives, processes and mapped ISO 17799 controls, which were identified as improvement opportunities. This report was called the IT Strategic Objective Plan (IT-SOP), since it contains only the relevant improvement opportunities for the district, incorporated into strategic implementation phases.

A detailed ISO 17799 / COBIT analysis was then conducted at the district municipality to identify which ISO 17799 controls were already implemented, partially implemented and which controls were not implemented at all. A survey and group interviews were used for this purpose and the following information was gathered:

- Which ISO controls were applicable to the district municipality;
- To which extent each applicable control was currently implemented;
- The improvement opportunities for each ISO 17799 control.

These ISO control results were combined with the IT-SOP and provided to the district municipality. This report contained the improvement opportunities for the district municipality for COBIT, as well as ISO 17799, tailored to their IT governance requirements. The IT-SOP was then accepted and approved by the municipal executive management as a means to introduce effective IT governance within the municipality and to mitigate the shortcomings as highlighted in the annual municipal IT audit reports. These reports should not be used as the only means for defining IT governance practices within the municipality. The following paragraphs state the reasons for this.

The yearly IT audit documents of the municipalities focus primarily around the following areas of IT governance (George Municipality, 2006):

- Planning, policies and procedures
- Implementing standards and Best Practices
- IT Continuity
- IT Documentation
- Security Controls

These audit reports also contain audit-related information regarding the financial systems. The IT audits are conducted before the financial information of municipalities is audited. However, good governance practices need to be implemented in order to comply with the areas of focus as mentioned, as well as to continue to govern the implemented procedures.

If the above mentioned areas are addressed on an ad-hoc basis (i.e. only implement controls and procedures when the audit documents require it), it will lead towards an unstructured IT governance approach. Therefore, the audit documents are valuable to determine how to satisfy regulatory requirements as set out in the law, but it cannot be used as the only source of information on the governance of Information

Technology.

Good IT governance practices can be compared to a healthy, balanced diet. By giving attention to all areas of a diet will create a healthy environment for the human body to function – by keeping fit and preventing illness from occurring. Audit reports can be compared to a doctor's assessment; to observe to see if everything is in order, provide recommendations on exercise, diet and other health-related issues for areas of concern. Similarly, good IT governance practices will create a 'healthy' environment for the IT functions to continually operate effectively. It is important for municipalities to prevent IT governance-related issues from occurring, rather than to wait until they have been identified in a yearly audit. Audit reports should therefore not be used to address the 'symptoms' of bad practices, but rather to assist in ensuring that a good governance plan is on track.

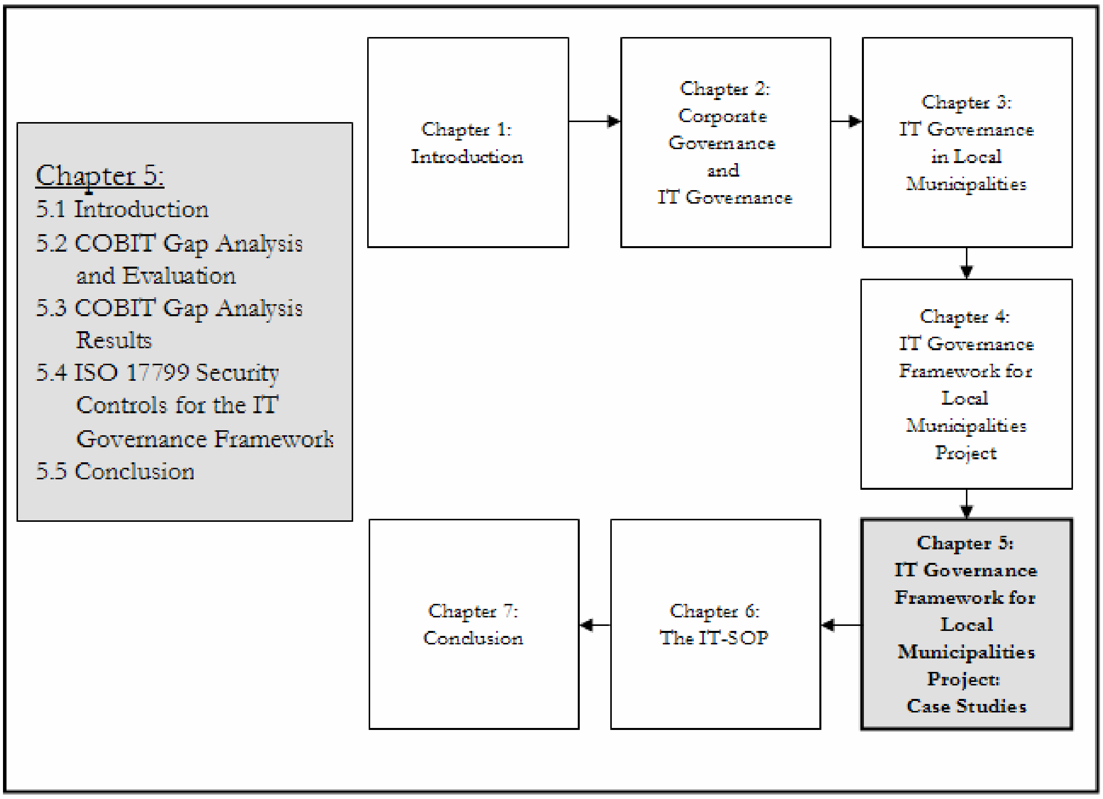
The shortcomings highlighted in the audit reports are not only addressed by implementing the proposed framework, but are also surpassed as they enable the municipality to have sound IT governance practices and an IT infrastructure that reflect the strategic requirements of the municipality.

4.6 Conclusion

There are various factors that contributed to the current state of IT governance within local municipalities and to this project. It is clear that a proper IT governance framework is required for municipalities. There are various possible IT governance frameworks, but COBIT was chosen, since municipalities are audited against COBIT on an annual basis. Poole's governance approach was combined with the IT governance implementation guide to provide the required, combined implementation approach. Case studies were conducted at the district and the underlying municipalities in order to determine the requirements of the implementation project, as well as what the current state of implementation maturity is, and what the target maturity levels are for every relevant COBIT objective. The results were communicated to the municipalities in the form of reports. These individual results were combined to produce a holistic, district-wide view of the current state of IT governance within the municipalities. The IT-SOP was produced and supplied to the district municipality. This report contained the improvement opportunities for the relevant COBIT processes, as well being segregated into strategic implementation phases. The details of the case studies from the district and underlying local municipalities are discussed in the next chapter.

Chapter 5

IT Governance Framework for Local Municipalities Project: Case Studies


Chapter 5:
5.1 Introduction
5.2 COBIT Gap Analysis and Evaluation
5.3 COBIT Gap Analysis Results
5.4 ISO 17799 Security Controls for the IT Governance Framework
5.5 Conclusion
Chapter 1: Introduction
Chapter 2: Corporate Governance and IT Governance
Chapter 3: IT Governance in Local Municipalities
Chapter 4: IT Governance Framework for Local Municipalities Project
Chapter 5: IT Governance Framework for Local Municipalities Project: Case Studies
Chapter 6: The IT-SOP
Chapter 7: Conclusion

5.1 Introduction

An investigation of the current status of IT governance at the target group of municipalities was required in order to accurately define an IT governance framework for them. It was, therefore, required to perform case studies at all of the local municipalities involved. These case studies included the use of questionnaires, individual interviews as well as group interviews in order to obtain the most meaningful input information and results.

This chapter discusses the case studies that were conducted at the various participating local municipalities. The research methods employed, as well as examples of how these tools were used are examined and examples are provided. The research process of conducting the case studies, the results and how the results from the various local municipalities were combined are investigated. The COBIT gap analysis is examined first, after which the results and the consolidating of the results into a single result follows. To complete the chapter, the linking of the ISO 17799 security standard with the COBIT results is discussed.

5.2 COBIT Gap Analysis and Evaluation

A COBIT gap analysis was conducted at a District municipality and its underlying local municipalities. The objective of the gap analysis was to determine the requirements for the IT governance framework for local municipalities. These requirements to be determined were:

- which COBIT objectives and processes are relevant to local municipalities;
- what the minimum acceptable (desired) maturity level is for each of the relevant objectives (to-be);
- what the current maturity level is for each of the relevant objectives (as-is).

COBIT's structure, as discussed in Chapter 3, contains more than 300 detailed control objectives. These detailed objectives span over 34 high-level objectives and are grouped into four domains: Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS) and Monitor (M). These high-level objectives and their respective detailed control objectives were evaluated in the project.

At each municipality listed above, a live case study was performed, which included a questionnaire which was completed with the use of interviews. The questionnaire contained the four COBIT domains, the 34 high-level objectives and their respective detailed control objectives. Each of the objectives was discussed to determine the relevance, as well as the minimum acceptable (to-be), or target maturity level for each relevant objective. The questionnaires were compiled from the COBIT control objectives (IT Governance, 2007b), formulated as questions. These questionnaires were completed as a group and the average duration for the completion of these questionnaires was two days during office hours. The participants spanned personnel from IT management, as well as from the human-resources departments. The respondents were given an induction into the questionnaire process and the importance thereof. Group dynamics were efficient, as all of the participants were granted time to voice their opinions and a general consensus was reached for every discussion. The maturity model of each objective, as well as the audit reports' specific requirements were consulted for this purpose. Since the audit process was conducted using COBIT as well, there were clear links as to which audit report requirement belonged to which COBIT high-level objective. The audit report maturity requirement was accepted as the minimum maturity level, but in most cases, the minimum maturity level was accepted by the municipality at a higher level than that which the audit report required. The detailed control objectives were then evaluated against the generic maturity model to gain understanding of how each detailed objective is currently implemented in the municipality. The evaluated maturities of the detailed control objectives then gave an indication as to the overall current maturity levels of the high-level objectives to which they belong. The results of these case studies are discussed in the next section.

5.3 COBIT Gap Analysis Results

To understand how each COBIT objective was evaluated in order to determine the target maturity level, the following example is provided. For illustrative purposes, an extract from the audit report of one of the local municipalities, LM1, (Mossel Bay Municipality, 2005, Page 6) is provided. The requirement and audit finding of disaster recovery and business continuity is stipulated in the report as follows: "A disaster recovery plan (DRP) or business continuity plan (BCP) have not been developed, documented and formally approved." It further states (in the recommendation section of the report) that, "The DRP and BCP should be tested on a regular basis and updated as necessitated by circumstances”. In terms of the maturity model, this shortcoming requires a documented and approved plan which should be tested and updated on a regular basis. The documented and approved procedure conforms to the fourth maturity level at which processes are documented, approved and communicated. However, the regular test and update procedures escalate the maturity model requirement to the fifth, Managed and Measurable, maturity level. This maturity level was set as the minimum acceptable level, which could further be escalated to level 5, the highest maturity level, if deemed necessary by the municipality. The questions regarding the detailed control objectives for DS4 in the questionnaire are provided in Table 5.1, in order to understand how the current maturity level for each detailed control objective was evaluated.

Table 5.1: Questionnaire Excerpt for DS4: Ensuring Continuous Service Objective

Business Process:	**(DS4) Ensure continuous service**						
Business Need:	IT services are available as required and to ensure a minimum business impact in the event of a major disruption						
#	Question	Response					
21.1	Have IT management and business process owners established a continuity framework which defines the roles, responsibilities and the risk-based approach/methodology to be adopted, and the rules and structures to document the continuity plan as well as the approval procedures?	0	1	2	3	4	5
21.2	Is the IT continuity plan in line with the overall business continuity plan to ensure consistency? Furthermore, does the IT continuity plan take into account the IT long- and short-range plans to ensure consistency?	0	1	2	3	4	5
21.3	Has IT management developed a written plan containing the following: • Guidelines on how to use the continuity plan? • Emergency procedures to ensure the safety of all affected staff members?	0	1	2	3	4	5

	• Response procedures meant to bring the business back to the state it was in before the incident or disaster? • Recovery procedures meant to bring the business back to the state it was in before the incident or disaster? • Procedures to safeguard and reconstruct the home site? • Co-ordination procedures with public authorities? • Communication procedures with stakeholders, employees, key customers, critical suppliers, stockholders and management? • Critical information on continuity teams, affected staff, customers, suppliers, public, authorities and media?						
21.4	Have procedures and guidelines been established for minimizing the continuity requirements with regard to personnel, facilities, hardware, software, equipment, forms, supplies and furniture?	0	1	2	3	4	5
…	…	…	…	…	…	…	…
21.14	How relevant is this IT process to your organization?	0	1	2	3	4	5

IT Management at Mossel Bay indicated that according to them, this objective's target maturity should be set at level five. Therefore, question 21.14 was responded to with a five. Table 5.2 provides the responses to the questions for DS4.

Table 5.2: Responses to Questions of DS4

21.1	2
21.2	2
21.3	2
21.4	1
21.5	1
21.6	1
21.7	1

21.8	1
21.9	1
21.10	1
21.11	1
21.12	2
21.13	1
21.14	5

Questions 21.1 to 21.13 were directed at the 13 detail control objectives of DS4, while 21.14 indicated the minimum acceptable maturity level for this objective. From the responses gathered for this objective (the as-is and to-be levels), it was possible to calculate the gap that exists. Figure 5.1 graphically depicts the responses versus the target maturity level. The black bars indicate COBIT maturity level 5, the highest maturity level, while the blue bars indicate the target maturity level for the objective and the red bars indicate the current (as-is) maturity level for each detail control objective for DS4.

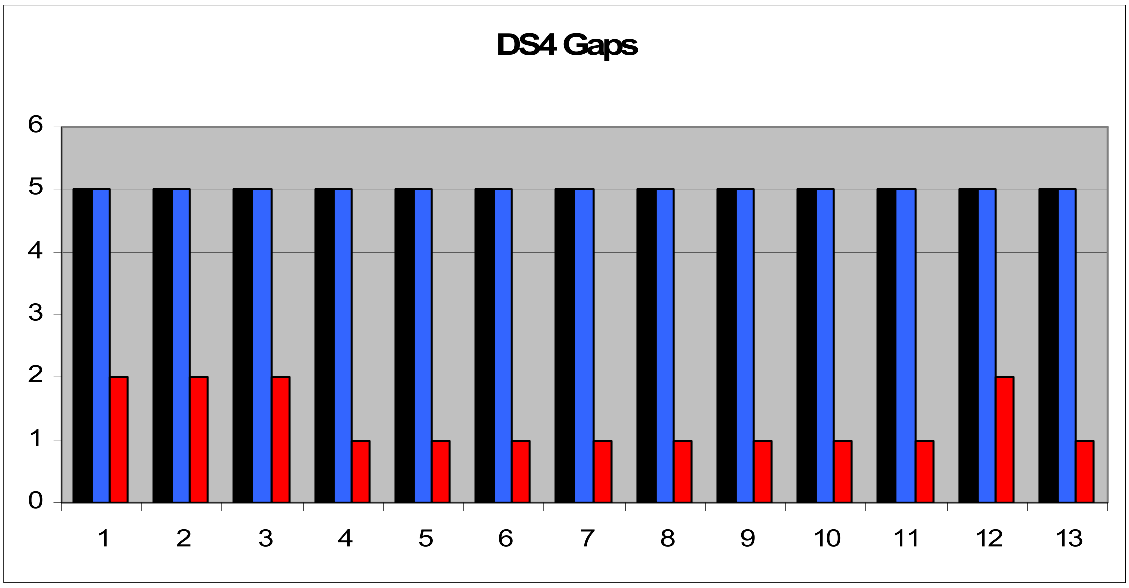


Figure 5.1: The Current (As-Is) Versus the Target Maturity Levels for DS4

The as-is bars were colour-coded (shaded) according to the following criteria. If the gap between the target maturity level and the detail control objective's maturity level is greater than 50%, then the as-is bar is red (depicted in Figure 5.1 above), indicating a severe risk. If the gap is between 35% and 50%, then the as-is bar is shaded in orange. If the gap is between 15% and 35%, then the as-is bar is shaded in yellow. For gaps smaller than 15%, the as-is bar is shaded in green, indicating a low risk.

The average of all of the as-is responses provides an indication of the current maturity level of the DS4 objective. Thus, the sum of the responses to questions 21.1 to 21.13, divided by 13 equals 1.31. This number indicates that the DS4 objective is, in totality, implemented at a maturity level between levels 1 and 2. Thus, a gap of 5 – 1.31 = 3.69 maturity level differences exists for this objective. This gap value was then expressed as a percentage value, which is more meaningful. Therefore, the gap percentage is calculated as 100 – (1.31/5*100) = 73.8% gap. Once the percentages were calculated for all relevant objectives for the DS domain, the average of these objectives provides an indication of the gap percentage for the DS domain. The average of the gap percentages of the four domains then provides an overall gap percentage for the current implementation of COBIT within the municipality. However, since the averaging of averages may result in the loss of accuracy, the gap for each detail control objective was measured on a points basis as well. For instance, if the target level is 5 and the current level is 1, then the gap is 4 points. Following this scoring method, DS4 scored 17 points out of a target score of 65 points, producing a 73.85% gap. The DS domain, in turn, scored 282 out of 569 points (50.44% gap), while the overall score for the four domains was 644 points out of a target score of 1293 points (50.2% gap). The detail results (graphs) are attached as an appendix at the end of the dissertation. Chapter 6 provides more detail regarding the origin and development of the tool.

It is not an objective of this project to perform mathematical or statistical analysis on the captured data from the municipalities. The relevant COBIT objectives, as well as the minimum acceptable maturity levels for each of these objectives were required to compile the proposed IT governance framework. The current maturity levels (as-is) and the calculated gaps were used to report on the current level of IT governance within each municipality. This report would serve the purpose of creating awareness of the current state of IT governance in the municipality, in terms of COBIT and the target maturity levels, as indicated by the municipality itself. It was also a token of gratitude for the participation of the municipality in the IT governance framework project. The gap analysis phase of the project can be summarized as follows:

- identify the relevancy of each high-level objective with the use of interviews and the audit reports;
- identify the minimum acceptable (as-is) maturity level for each relevant high-level objective with the use of interviews, the objective's maturity model and the audit reports;
- identify the current maturity level for each relevant high-level objective's detailed

control objectives with the use of interviews and the generic maturity model;

- calculate the gap between the as-is and to-be maturity levels and present this gap as a percentage for the COBIT objective, domain and overall implementation.

The next step towards the IT governance framework was to combine the target maturity levels from all the municipalities. These consolidated maturity levels then served as the district-wide benchmark or minimum acceptable maturity levels and also the basis for the IT governance framework for local municipalities.

The process of consolidating the target maturity levels were as follows. During a meeting at the Eden District Municipality, the target maturity levels were discussed with the participating municipalities' IT management. Each relevant objective was evaluated and the target maturity level which was in the majority was then chosen as the district-wide target maturity level for the objective. Table 5.3 depicts the consolidated target maturity levels, which were the result of various meetings.

Table 5.3: The Consolidated Target Maturity Levels for the COBIT Objectives

Domain / Objective	1	2	3	4	5	6	7	8	9	10	11	12	13
PO	4	4	4	4	4	4	4	4	4	4	4		
AI	4	4	4	4	4	4							
DS	4	4	4	4	5	3	4	4	4	4	5	4	4
M	4	4	4	4									

There are two conclusions which can be drawn from table 5.3. These are:

1. All of the COBIT objectives were relevant to the operating environment of a local municipality. Even though some of the objectives were not mentioned as a requirement in audit reports, the municipalities indicated that they were still relevant to them and needed to be addressed.
2. Not all of the objectives were required to be implemented at maturity level 5. The target maturity level for the majority of the objectives was set at level 4, with the exception of DS5, DS6 and DS11, which were set at levels five, three and five, respectively.

In order to remain current, the gap analysis results from the municipalities' case studies were amended to include the district-wide target maturity levels as a benchmark, rather than the target maturity levels as decided upon by the municipality involved. These new results served as an indication as to how they measure against the district-wide norm, as well as against their own acceptable levels.

Chapter 3 discussed the ISO 17799 standard for information security and how it complements COBIT. After the consolidated COBIT objectives' maturity levels were identified, the relevant security controls from ISO 17799 were incorporated into the proposed framework.

5.4 ISO 17799 Security Controls for the IT Governance Framework

The ISO 17799 controls were combined with the relevant COBIT objectives to enhance the value of the IT governance framework for local municipalities. This was performed after an ISO 17799 / COBIT mapping analysis study at the Eden District Municipality.

The purpose of this study, as discussed in Chapter 4, was to determine which ISO 17799 controls are applicable to a municipality, as well as which of these identified controls are linked to which COBIT objectives. The IT Governance Institute (2004) published the *COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT* document, which was used for this purpose. This document provides information on which ISO 17799:2000 security category maps to which corresponding COBIT (version 3) objective and which ISO 17799 security controls are related to which COBIT detail control objective. As stated earlier, COBIT version 3 was used for this project since version 4 was only published after the case studies were completed. However, ISO 17799:2005 were used for the security controls for the IT governance framework project. Therefore, after mapping the ISO 17799:2000 controls to COBIT, it was further required to map the ISO 17799:2000 controls to those of ISO 17799:2005. To achieve this, the *ISO 17799:2000 and ISO 17799:2005 Mapping of Security Categories between 2000/2005* document (17799.com, 2006) was consulted.

The process to obtain the ISO 17799 controls for the IT governance framework project was performed as follows. The ISO 17799 standard (Standards South Africa, 2005a, page xi) states that it is not required for all of the listed controls to be implemented, since they might not all be applicable to a municipality. However, it lists three controls (Standards South Africa, 2005a, page x) which are fundamental and are considered essential from a legislative perspective. These controls are:

1. the protection of data and privacy of personal information;
2. the protection of organisational records;
3. intellectual property rights.

It further states that the following seven controls are considered to be "common practice" in organisations where good information security governance is exercised:

1. information security policy document;
2. allocation of information security responsibilities to organisational entities;
3. information security awareness, education and training;
4. the correct processing in applications;
5. technical vulnerability management;
6. business continuity management;
7. management of information security incidents and improvements.

The standard describes these above-mentioned controls as being "applicable to most organisations in most environments". Thus, these controls were stated as being mandatory for municipalities as well. Any other control, except for these mandatory controls, could therefore be identified as not being applicable to the municipality. The list of security controls from the 2005 edition (Standards South Africa, 2005b) were compiled into a questionnaire and discussed during a group interview. This questionnaire took three days to complete and was completed in a similar fashion of the COBIT questionnaires.

For each security control, a response was obtained to determine if the control is applicable to the municipality and to what extent it had been implemented. Questions could be responded to as either one of the following states:

- 0: Not implemented at all, but the control is applicable to the municipality and should be implemented at some stage;
- 0.5: The control is applicable to a municipality and has been implemented to a certain degree, but not to the full extent of which the ISO 17799 standard requires;
- 1: This control is applicable to a municipality and has been implemented to meet the requirements to the ISO 17799 standard;
- NA: This control is not applicable to a municipality and therefore is not required to be implemented.

This questionnaire produced a list of controls which is not applicable to the municipality. This list could possibly be used in future to formulate a statement of applicability when applying for possible ISO certification against the ISO 17799 standard. The questionnaire also produced a list of all the applicable controls, as well as which of these controls required improvements to be made. These improvement opportunities were then linked together with their corresponding COBIT objectives. The COBIT objectives and their linked ISO 17799 controls formed the basis for the IT-SOP, which is discussed in Chapter 6.

5.5 Conclusion

Case studies were employed as the primary research method in order to obtain the results required for the IT governance framework project. The case studies comprised of two questionnaires, one to determine the relevant COBIT objectives, the current and target maturity levels of the identified objectives and the second, to determine the applicable ISO 17799 security controls and their current levels of implementation.

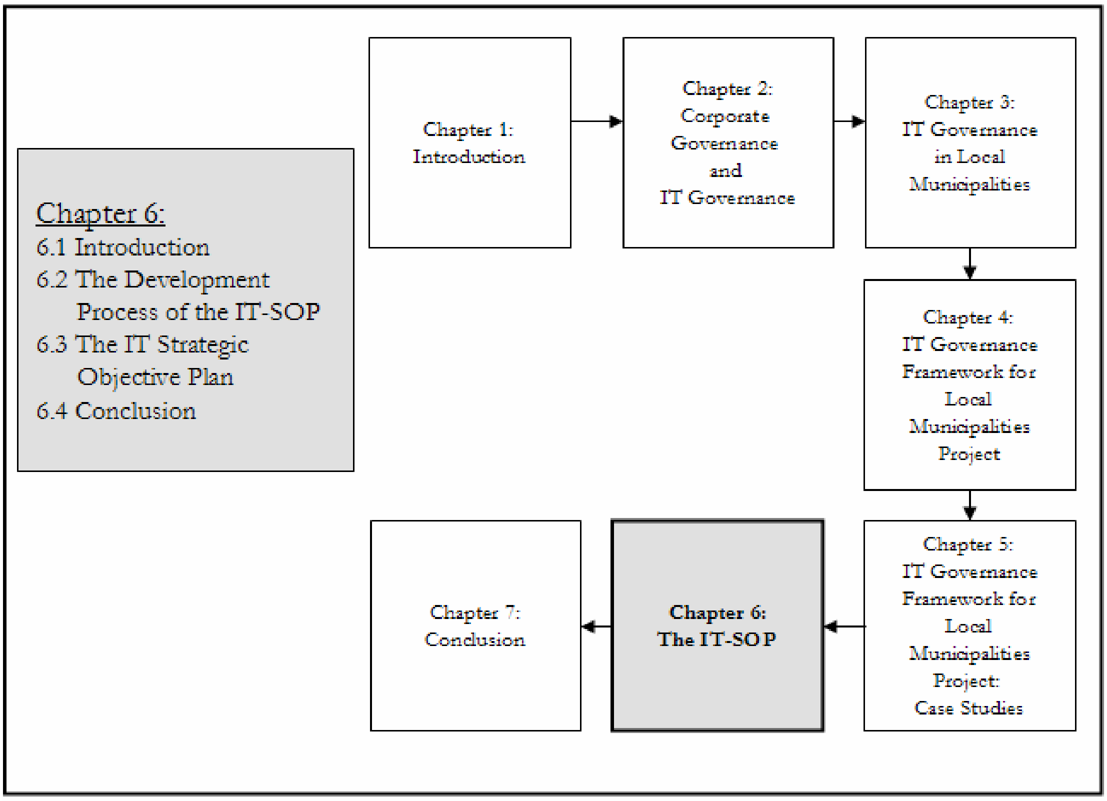
The COBIT questionnaire produced the relevant objectives and their minimum acceptable (target) maturity levels which were important for the IT governance framework project. It further produced the current maturity levels and the gaps between the current and target maturity levels. These gaps were used to identify improvement opportunities for the COBIT objectives and to provide the participating municipalities with a report on what the current state of IT governance, in terms of COBIT, is in their respective municipalities. The individual municipal results were combined and integrated into a single 'improvement strategy'. The improvement opportunities were prioritised and grouped into phases to assist the management and implementation thereof, as well as to improve the chance for the overall implementation strategy to be successful.

An ISO 17799 mapping analysis case study was then also performed to obtain which ISO 17799 controls were applicable to a local municipality, as well as to which extent the applicable controls were already implemented. The gaps were translated into improvement opportunities, and these controls were linked to their associated COBIT objectives in their respective phases within the overall improvement strategy. This overall improvement strategy was documented and called the IT Strategic Objective Plan (IT-

SOP). The IT-SOP is discussed in more detail in the next chapter.

Chapter 6

The IT Strategic Objective Plan (IT-SOP)


Chapter 6:
6.1 Introduction
6.2 The Development Process of the IT-SOP
6.3 The IT Strategic Objective Plan
6.4 Conclusion
Chapter 1: Introduction
Chapter 2: Corporate Governance and IT Governance
Chapter 3: IT Governance in Local Municipalities
Chapter 4: IT Governance Framework for Local Municipalities Project
Chapter 5: IT Governance Framework for Local Municipalities Project: Case Studies
Chapter 6: The IT-SOP
Chapter 7: Conclusion

6.1 Introduction

The IT-SOP is the main deliverable of this IT governance project, since it is the document which contains the IT governance framework for local municipalities, as derived from the results of the various studies explained in Chapter 5. This framework has been tailored to suit the requirements of all of the participating municipalities and has been based on the international best-practice COBIT and the ISO 17799 standard for information security management. The IT-SOP contains only the IT governance objectives (as per COBIT) and security controls (as per ISO 17799), which have been identified as requirements by the municipalities involved.

This chapter discusses the process of developing the IT-SOP, as well as the contents thereof, in terms of the way in which the identified COBIT objectives and associated ISO 17799 controls are integrated and grouped into each phase of the implementation strategy, as well as the project plan, which was developed to facilitate the implementation of the IT-SOP.

6.2 The Development Process of the IT-SOP

This section discusses the consolidation of all of the information that was gathered from all the various sources, into the IT-SOP. The IT-SOP, including its detailed project plan, is the main deliverable of the municipal IT governance research project. This project forms part of the wider project of which this dissertation (towards a master's degree) is the main deliverable. The objective of the IT-SOP will be discussed, after which the rest of the section provides a detailed description of the process followed towards the development of this IT governance framework.

The objective of the IT-SOP is to provide a district or local municipality with a strategic plan that enables the municipality to implement the international best practice, COBIT, as well as the ISO 17799 information security standard, which have both been tailored to suit the requirements of a municipality. The following sub-sections explain how this IT-SOP was developed.

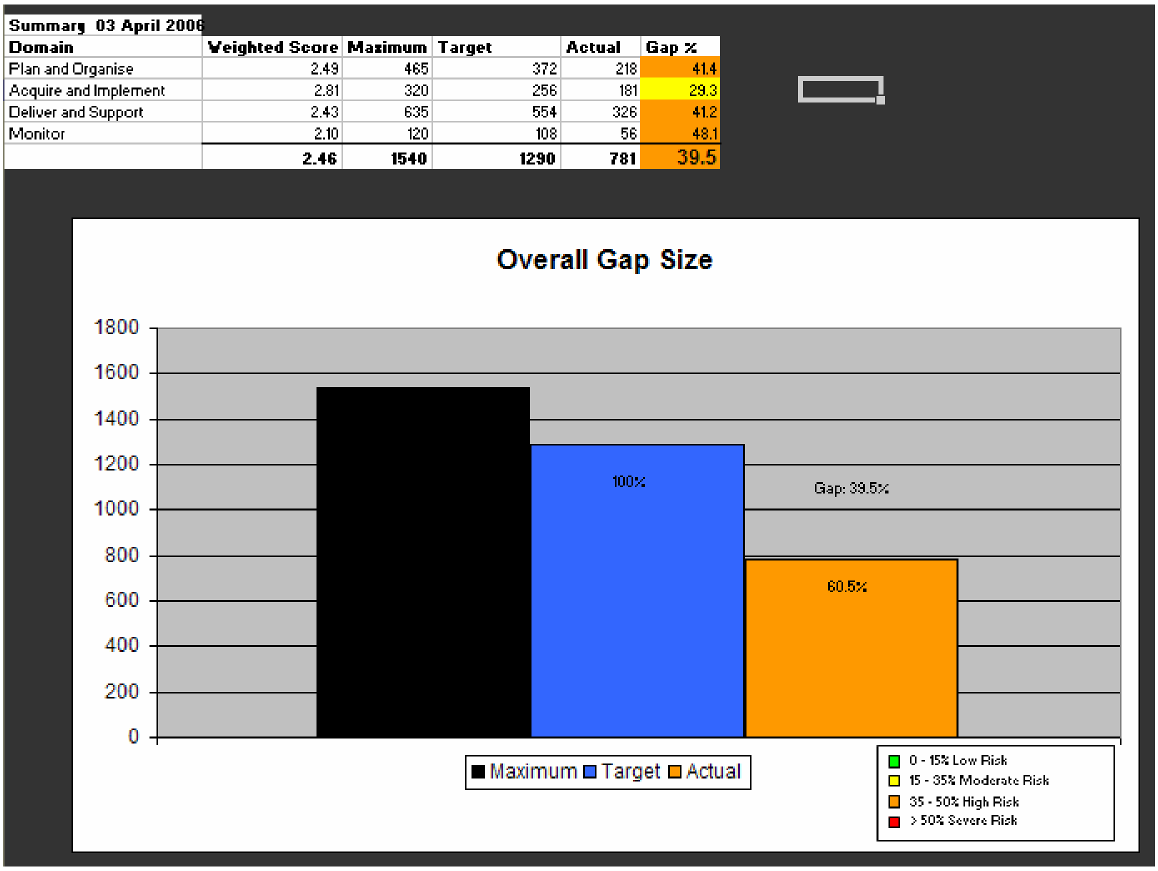
6.2.1 Initial Investigation and Proposal

An initial investigation was performed into the current state of IT governance within municipalities. An extensive literature survey was conducted to determine if there is currently any municipal legislation that prescribes how the IT infrastructure and systems of a municipality should be governed. Other governance and regulatory mandates, such as King II (King Report, 2002) and the Electronic Communications and Transactions Act (ECT Act, 2002), were also consulted to determine whether they stipulate any mandatory regulations aimed at municipalities. Media reports, which reported on typical IT governance problems that are currently experienced by municipalities, were also analysed and documented. After the initial literature research, an interview was conducted at the participating district municipality where it was noted that municipalities are audited on an annual basis against some of the objectives from the COBIT best practice framework. The objective of this interview was to create awareness in the IT function of the district municipality regarding sound IT governance and what it involves. During this interview, the municipal manager and IT manager expressed their desire to improve the governance of IT in the district municipality and all of the associated local municipalities. The COBIT best-practice framework and the ISO 17799 information security standard were introduced to the municipality as well. After this interview, the initial report was drafted and communicated to the district municipality. In this report, COBIT and ISO 17799, and how they contribute towards the surpassing of the annual audit reports and mitigate the current IT governance shortcomings, were introduced to the district and local municipalities. This report was called the business benefit report.

6.2.2 The COBIT Case Studies and Developed Tool

As stated in Chapter 5, the requirement for the IT governance framework was not to implement COBIT to its fullest extent, but to tailor it to suit the environment and the business requirements of the district and local municipalities. Therefore, case studies were planned as follows: firstly, a COBIT gap analysis had to be conducted at the district municipality and the underlying, local municipalities. The information to be gathered towards the IT-SOP was the COBIT objectives that are relevant to a municipality and the target maturity level for each of the identified COBIT objectives. For reporting and incentive purposes, a full gap analysis was performed at each municipality to provide them with information on what their current performance was regarding IT governance, when measured against each of the identified, target maturity levels. The gap analysis required a tool to analyse the current implementation maturity levels, against the target maturity levels. After an extensive market survey, no suitable tools could be identified to assist in this task. They were either inferior or very expensive as they provide a lot of information that is not relevant to this project. Therefore, it was decided to develop a tool to capture the gap-analysis data and present it in a meaningful format. Chapter 5 discussed results from the case studies and how they were gathered from the tool itself, but this section discusses how the tool functions. The following paragraphs describe the functioning of this tool.

The developed tool is used to calculate a risk percentage for IT governance within the municipality. This percentage is based on all of the COBIT control objectives, their importance to the municipality and the current level of compliance. The tool is structured as a hierarchy that represents the hierarchical structure of COBIT. The tool presents a high-level information screen, referred to as the dashboard. The dashboard displays gap information for the four COBIT domains: Plan and Organize, Acquire and Implement, Deliver and Support and Monitoring. The overall gap information is also displayed on the dashboard that consists of the combined gap information of the four domains. An example of the dashboard is depicted in Figure 6.1. An excerpt from the questionnaire that was used to gather the responses is appended to this dissertation as Appendix A and an example of this gap analysis tool is appended to this dissertation as Appendix B.

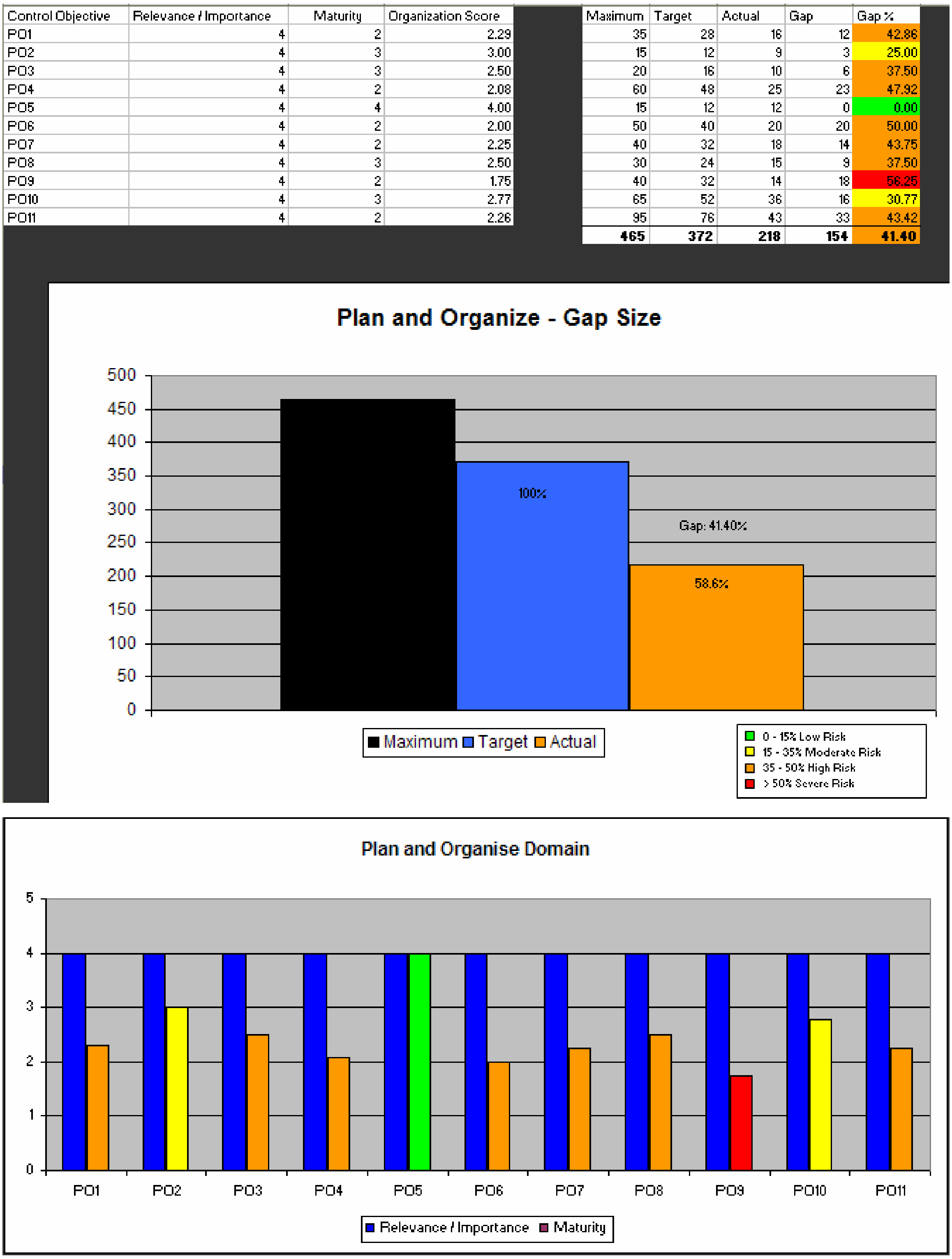


Summary 03 April 2006

Domain	Weighted Score	Maximum	Target	Actual	Gap %
Plan and Organise	2.49	465	372	218	41.4
Acquire and Implement	2.81	320	256	181	29.3
Deliver and Support	2.43	635	554	326	41.2
Monitor	2.10	120	108	56	48.1
	2.46	1540	1290	781	39.5

Figure 6.1: The Dashboard

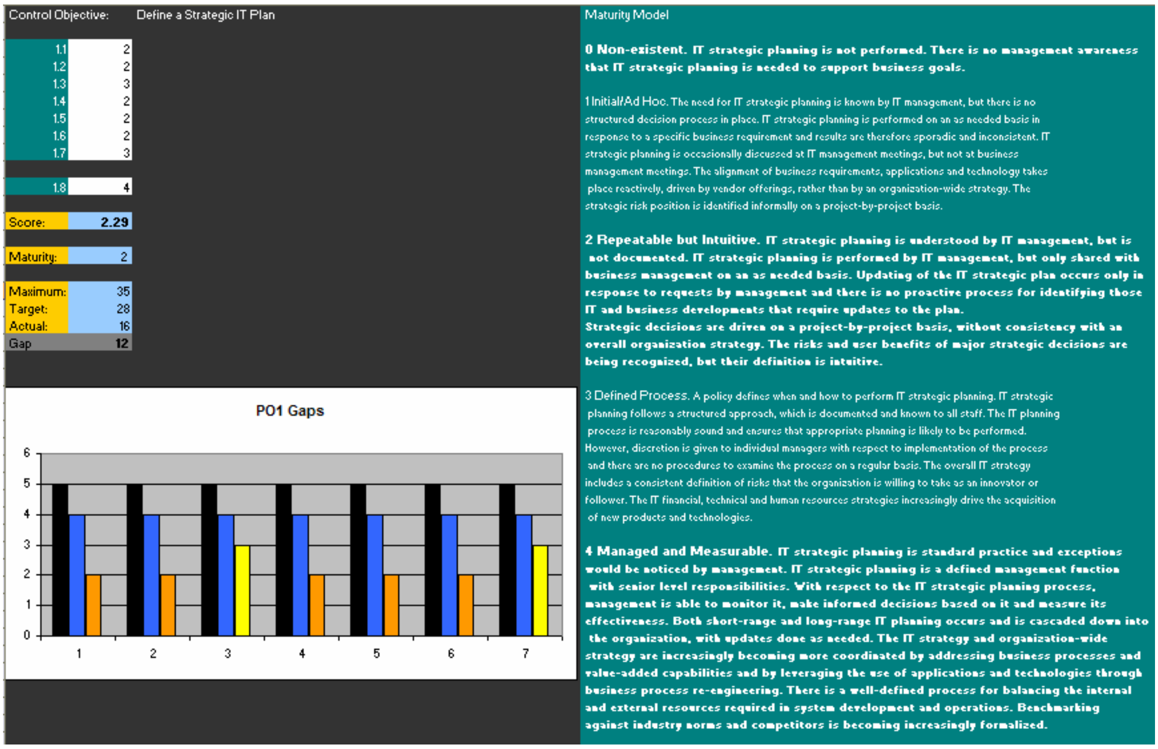
The next level in the tool's hierarchy is the four COBIT domains. The gap information for the Plan and Organize domain, for example, is shown in the Plan and Organize screen. Here, all of the objectives, their current maturity level, target maturity levels and gaps are shown. Figure 6.2 depicts this gap analysis screen for each COBIT domain.



Control Objective	Relevance / Importance	Maturity	Organization Score	Maximum	Target	Actual	Gap	Gap %
PO1	4	2	2.29	35	28	16	12	42.86
PO2	4	3	3.00	15	12	9	3	25.00
PO3	4	3	2.50	20	16	10	6	37.50
PO4	4	2	2.08	60	48	25	23	47.92
PO5	4	4	4.00	15	12	12	0	0.00
PO6	4	2	2.00	50	40	20	20	50.00
PO7	4	2	2.25	40	32	18	14	43.75
PO8	4	3	2.50	30	24	15	9	37.50
PO9	4	2	1.75	40	32	14	18	56.25
PO10	4	3	2.77	65	52	36	16	30.77
PO11	4	2	2.26	95	76	43	33	43.42
				465	**372**	**218**	**154**	**41.40**

Figure 6.2: Domain Gap Analysis

Further, the tool presents a screen to represent the recorded information for each of the 34 COBIT objectives. Each screen contains a description for each maturity level for the relevant objective's maturity, as well as data capture functionality for the detailed control objectives contained in the current COBIT objective. The data capture functionality is used to gather the current maturity level for each detail objective. Figure 6.3 provides an example of the data captured for every detailed control objective according to the generic maturity model as follows. If the detailed objective is not performed at all, a 0 (zero) is assigned to the control objective. If the objective is only performed on an *ad-hoc* basis, then a 1 is assigned, and so forth. The highest score that can be attained is a 5, meaning that this control objective is constantly refined and measured against a best practice. After this detailed control objective evaluation, the screen also captures the target maturity level, as indicated either by the audit reports, IT management personnel, or both. If the current objective is not applicable, then a zero is assigned to it. Any detailed control objective which has a current maturity level higher than the target maturity level is adjusted to have a maximum value equal to the identified target maturity level. If this is not performed, then the overall gap information of the current COBIT objective will present a false value to the gap calculation, as is described in the next sentence. An average from all of the captured, current maturity levels is calculated and compared against the identified target maturity level for the current COBIT objective. Figure 6.3 is an example screenshot of one of the reporting screens from the tool and should be interpreted with the tool.


Control Objective: Define a Strategic IT Plan

1.1	2
1.2	2
1.3	3
1.4	2
1.5	2
1.6	2
1.7	3
1.8	4
Score:	**2.29**
Maturity:	2
Maximum:	35
Target:	28
Actual:	16
Gap	**12**

Maturity Model

0 Non-existent. IT strategic planning is not performed. There is no management awareness that IT strategic planning is needed to support business goals.

1 Initial/Ad Hoc. The need for IT strategic planning is known by IT management, but there is no structured decision process in place. IT strategic planning is performed on an as needed basis in response to a specific business requirement and results are therefore sporadic and inconsistent. IT strategic planning is occasionally discussed at IT management meetings, but not at business management meetings. The alignment of business requirements, applications and technology takes place reactively, driven by vendor offerings, rather than by an organization-wide strategy. The strategic risk position is identified informally on a project-by-project basis.

2 Repeatable but Intuitive. IT strategic planning is understood by IT management, but is not documented. IT strategic planning is performed by IT management, but only shared with business management on an as needed basis. Updating of the IT strategic plan occurs only in response to requests by management and there is no proactive process for identifying those IT and business developments that require updates to the plan.
Strategic decisions are driven on a project-by-project basis, without consistency with an overall organization strategy. The risks and user benefits of major strategic decisions are being recognized, but their definition is intuitive.

3 Defined Process. A policy defines when and how to perform IT strategic planning. IT strategic planning follows a structured approach, which 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 on a regular basis. The overall IT strategy includes a consistent definition of risks that the organization is willing to take as an innovator or follower. The IT financial, technical and human resources strategies increasingly drive the acquisition of new products and technologies.

4 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. With respect to the IT strategic planning process, management is able to monitor it, 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 organization, with updates done as needed. The IT strategy and organization-wide strategy are increasingly becoming more coordinated by addressing business processes and value-added capabilities and by leveraging the use of applications and technologies through business process re-engineering. There is a well-defined process for balancing the internal and external resources required in system development and operations. Benchmarking against industry norms and competitors is becoming increasingly formalized.

Figure 6.3: The Detail Control Objective Screen

For the seven Plan and Organize high level objectives, all are ideally set to function on maturity level 4 (The blue bars). The current maturity levels are presented by the third bar respectively, for example, for objective 1 (of PO1) the current maturity level is 2. If the current, calculated maturity level is within 15% of the target maturity level, the current level is represented by a green bar. If they differ by between 15% and 35%, it is represented by a yellow bar, between 35% and 50%, an orange bar and by more than 50%, a red bar. The power of this tool lies with the hierarchical structure and how the data from one level is combined and displayed at the higher level, while being combined here again and displayed at its higher level, until it is displayed on the dashboard (see Figure 6.1). For example, the gaps and scores of all four COBIT domains show on the dashboard and this information is then used to calculate the overall gap percentage.

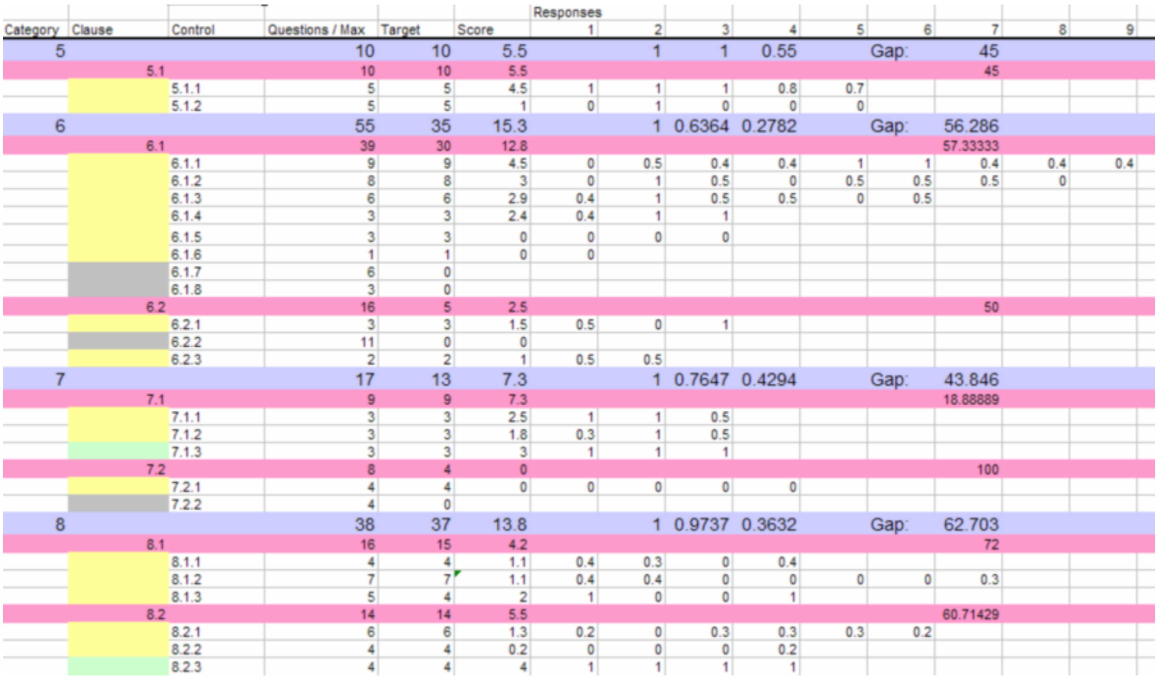
This tool provided the case studies with the required information to determine the COBIT objectives that are relevant to the municipality, the current maturity levels for every identified COBIT objective and the target maturity level for every identified COBIT objective. The gaps could then be determined by comparing the current maturity level to that of the identified target maturity level. The results from the case studies and the identified gaps were then presented to the IT function of each municipality. During this presentation, the IT managers from all the local municipalities, as well as from the district municipality, were present.

As discussed in Chapter 5, the results from the various municipalities were then integrated and the district-wide maturity level was then produced, which is the basis for the IT-SOP. The next step in the development of the IT-SOP was to determine the relevant ISO 17799 information security controls, and which of these identified controls required further improvement for full implementation, which is discussed next.

6.2.3 Determining the Relevant ISO 17799 Security Controls

The relevant ISO 17799 information security controls were gathered using the same approach as for the COBIT objectives. A questionnaire and tool were developed to gather the applicable ISO 17799 controls for a municipality, as well as the implementation level for each identified control. The main difference between the COBIT gap analysis and the ISO 17799 analysis is that COBIT uses its maturity model to gauge implementation, whereas with ISO 17799, a control can only by implemented to its specification, be partially implemented, or not implemented at all. These three states were used as a metric to gauge levels of implementation.

The developed ISO 17799 gap analysis tool enabled the municipality to identify the applicability of each ISO 17799 control with a score of 1, whereas non-applicable is indicated as a zero. For every control, questions were developed for each specification requirement within the control. If the requirement was implemented to the specification of ISO 17799, then the implementation score for the requirement is 1. If the requirement has not been implemented, then a score of 0 is assigned. A partial implementation constitutes a requirement that has been implemented, but might not be to the extent of the 17799 specification. In such a case, a value between 0 and 1 is determined that is representative of the extent to which the requirement is implemented to the 17799 specification. For example, if a control is implemented to only 80% of the ISO 17799 specification after careful consideration of the ISO 17799 control specification and the debate with the municipality, then an implementation score of 0.8 is assigned to the control, leaving a gap of 0.2 points. If there are five specification requirements per control, then the implementation for the control can score a maximum of five points. The implementation scores for these five requirements add up to produce the implementation score for the control. A screenshot of the scoring tool is provided in Figure 6.4



						Responses								
Category	Clause	Control	Questions / Max	Target	Score	1	2	3	4	5	6	7	8	9
5			10	10	5.5		1	1	0.55		Gap:	45		
	5.1		10	10	5.5							45		
		5.1.1	5	5	4.5	1	1	1	0.8	0.7				
		5.1.2	5	5	1	0	1	0	0	0				
6			55	35	15.3		1	0.6364	0.2782		Gap:	56.286		
	6.1		39	30	12.8							57.33333		
		6.1.1	9	9	4.5	0	0.5	0.4	0.4	1	1	0.4	0.4	0.4
		6.1.2	8	8	3	0	1	0.5	0	0.5	0.5	0.5	0	
		6.1.3	6	6	2.9	0.4	1	0.5	0.5	0	0.5			
		6.1.4	3	3	2.4	0.4	1	1						
		6.1.5	3	3	0	0	0	0						
		6.1.6	1	1	0	0								
		6.1.7	6	0										
		6.1.8	3	0										
	6.2		16	5	2.5							50		
		6.2.1	3	3	1.5	0.5	0	1						
		6.2.2	11	0	0									
		6.2.3	2	2	1	0.5	0.5							
7			17	13	7.3		1	0.7647	0.4294		Gap:	43.846		
	7.1		9	9	7.3							18.88889		
		7.1.1	3	3	2.5	1	1	0.5						
		7.1.2	3	3	1.8	0.3	1	0.5						
		7.1.3	3	3	3	1	1	1						
	7.2		8	4	0							100		
		7.2.1	4	4	0	0	0	0	0					
		7.2.2	4	0										
8			38	37	13.8		1	0.9737	0.3632		Gap:	62.703		
	8.1		16	15	4.2							72		
		8.1.1	4	4	1.1	0.4	0.3	0	0.4					
		8.1.2	7	7	1.1	0.4	0.4	0	0	0	0	0.3		
		8.1.3	5	4	2	1	0	0	1					
	8.2		14	14	5.5							60.71429		
		8.2.1	6	6	1.3	0.2	0	0.3	0.3	0.3	0.2			
		8.2.2	4	4	0.2	0	0	0	0.2					
		8.2.3	4	4	4	1	1	1	1					

Figure 6.4: The ISO 17799 Gap Analysis Tool

Referring to Figure 6.4 above, it is possible to see that for clause 6.2, for example, there are three controls, but 6.2.2's target score has been set at 0. This indicated that the control is not applicable. Therefore, it has been coloured grey in the second column. Green colouring, as can be seen for control 8.2.3, indicates that this control has been implemented to the full ISO 17799 specification. Yellow colouring indicates that the control is applicable but not yet to the ISO 17799 specification and requires improvement. The control totals add up to provide the implementation levels of the clause, which in turn add up to the implementation total for the security category. This analysis provided all of the ISO 17799 controls that require further improvement by the municipality, disregarding any ISO 17799 control that is either not applicable and requires no implementation, or has been fully implemented and also requires no further improvement. Thus, only the required ISO 17799 controls were identified for the next step, mapping the ISO 17799 controls to the COBIT objectives. The results of the ISO 17799 analysis were again presented to the district municipality during which the municipal manager and IT management were present. The questionnaire used for the ISO 17799 analysis is appended to this dissertation as Appendix C and the ISO 17799 analysis tool is appended as Appendix D.

6.2.4 Mapping the ISO 17799 Security Controls to COBIT

ISACA (IT Governance Institute, 2004) published the "*Mapping: Mapping ISO/IEC 17799:2000 to COBIT*" document, as referred to in Chapter 3. This document directly links each ISO 17799 security control to one or more COBIT objectives. Using this document, only the required ISO 17799 security controls were mapped to the COBIT objectives, disregarding the controls that were considered to be not applicable or fully implemented. The COBIT objectives, their KPIs, KGIs, and CSFs, the description of the target maturity level and the mapped ISO 17799 security controls were then integrated to eventually form the basis of the IT-SOP. The conceptual flow of the project, as described earlier, can be summarized and depicted as in Figure 6.5, which contains the literature surveys, case studies and each study's deliverables (oval shape).

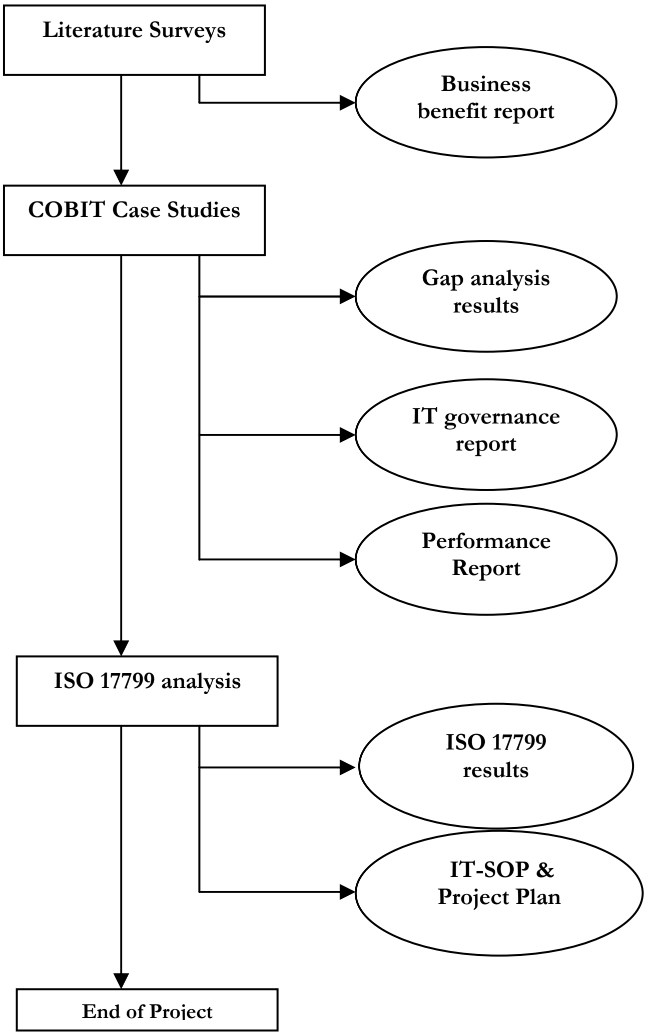


Figure 6.5: The Flow of the IT Governance Project

6.3 The IT Strategic Objective Plan (IT-SOP)

The IT-SOP is a strategic IT governance plan that should (once implemented) adhere to sound IT governance practices according to the international best practice, COBIT. The IT-SOP should ideally identify all COBIT objectives that are applicable to a district or local municipality as well as the maturity levels that best fit the implementation of each of these COBIT objectives. As the identified COBIT objectives to implement will be quite extensive, the IT-SOP makes provision for a number of implementation phases. Further, as information security forms an important part of the IT-SOP, each COBIT objective identified needs to be mapped to relevant ISO 17799 security controls. Also, the IT-SOP will be a very extensive strategic plan; therefore, a detailed project implementation plan also needs to form part of the eventual plan.

The eventual IT-SOP is the result of a number of case studies performed at the district municipality and its underlying local municipalities, as described above. It was compiled by combining the identified COBIT objectives from the individual case studies and the mapped ISO 17799 information security controls. These objectives were then prioritised, taking the audit reports' requirements, priorities highlighted by each municipality, as well as the current gap between each objective's target and current level of maturity. This plan is strategic by nature, since it only contains the relevant COBIT objectives and their mapped ISO 17799 controls, as well as only the necessary improvements which should be implemented as part of the overall improvement strategy. Each COBIT objective contains the following information:

- The maturity model for the objective, providing a description for each maturity level aimed at the objective;
- The current maturity level for the objective;
- The indicated target maturity level for the objective;
- An implementation guide of what needs to be done in order to advance the maturity for the objective to the target maturity level;
- The Critical Success Factors which are key to the success of the objective's implementation;
- Key Goal Indicators and Key Performance Indicators, which can be used to determine whether the objective's implementation has indeed reached its goal and to measure if the performance levels of the objective are satisfactory;
- The mapped ISO 17799 security controls, which were partially, or not at all implemented by the municipality. If the ISO 17799 control has already been mapped to a COBIT objective in the current or a previous implementation phase, then it is regarded as already implemented by the time that the current objective is to be implemented.

The COBIT objectives identified plus the associated ISO 17799 controls were then grouped into phases: each phase containing between four and six objectives and the mapped ISO 17799 controls.

There are many instances where one ISO 17799 control is mapped to multiple COBIT objectives. Since it is only required to implement an ISO 17799 control once in an organisation, the redundant control mappings of ISO controls in subsequent phases were ignored. The end result was a strategic IT plan for the implementation of IT governance within a municipality, which is tailored to the requirements of municipalities involved, that surpasses the shortcomings highlighted in the annual audit reports from all of the municipalities involved in the project, and is based on internationally accepted best practices.

The proposed IT-SOP consists of four phases, three of which have been prescribed to the municipalities as non-negotiable. The fourth phase consists of the rest of the COBIT objectives, which also require improvement, but which have been given a lower priority ranking. After implementing the first three phases of the IT-SOP, it is then the responsibility of the municipality to define additional phases which group together the remaining COBIT objectives and ISO 17799 controls. Thus, the IT-SOP provides guidance to the municipality to implement the more critical COBIT objectives and ISO 17799 controls in the beginning phases. This ensures that a proper foundation for IT governance is put into practice at the beginning of implementation. The time and resources required to implement such a plan are considered to be fairly extensive; therefore, it is the responsibility of the municipality to decide on a time-frame, budget and resource allocation in order for the implementation of the IT-SOP to be successful. The four phases (main bullets) in the following list, their respective COBIT objectives (1st sub-level bullets), target maturity models in brackets and associated ISO 17799 controls (2nd sub-level bullets) are:

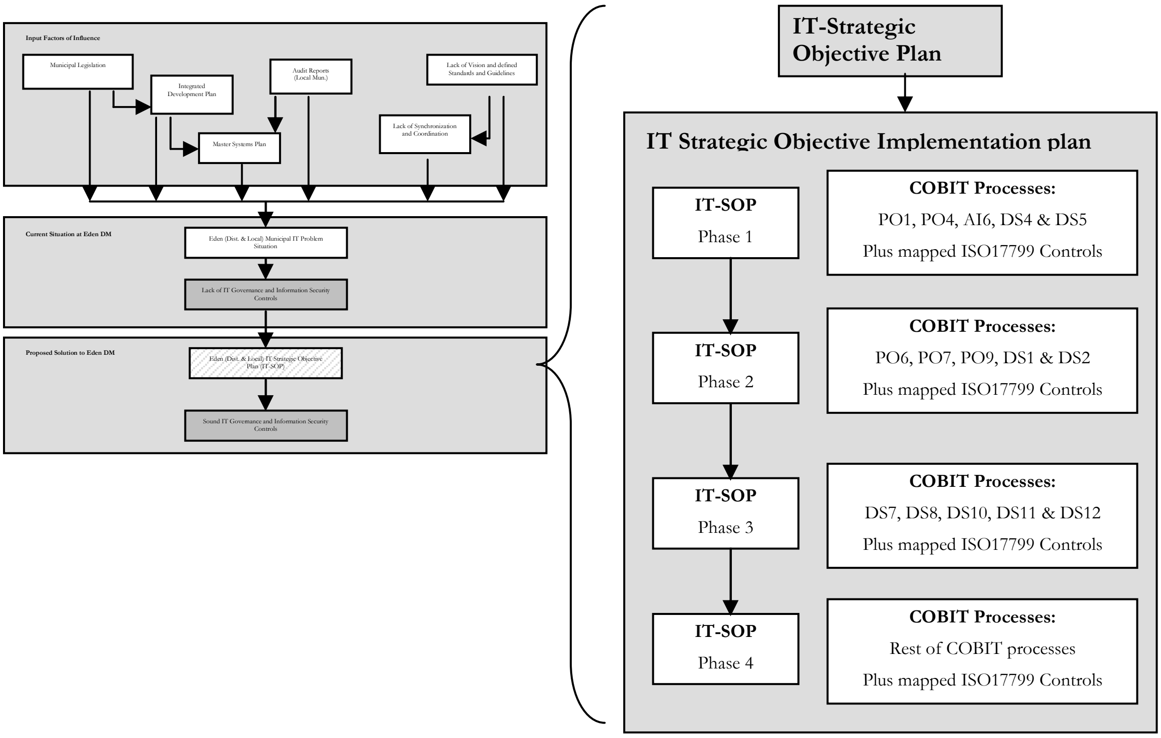
- Phase 1:
    - PO1 (Target Maturity Level 4)
        - No associated ISO 17799 controls
    - PO4 (Target Maturity Level 4)
        - Controls 6.1.1 to 6.1.6
        - Controls 6.2.1 and 6.2.2
        - Controls 7.1.1 and 7.1.2
        - Controls 8.1.1 to 8.1.3
        - Controls 8.2.1 and 8.2.2
        - Control 10.10.2
    - AI6 (Target Maturity Level 4)
        - Control 12.5.1
    - DS4 (Target Maturity Level 4)
        - Controls 14.1.1 to 14.1.5
        - Controls 9.2.1 to 9.2.7

  - DS5 (Target Maturity Level 5)
    - Controls 5.1.1 and 5.1.2
    - Control 6.2.3
    - Control 7.2.1
    - Controls 9.1.2, 9.1.3 and 9.1.5
    - Control 10.4.1
    - Controls 10.7.1, 10.7.3 and 10.7.4
    - Control 10.8.1
    - Controls 10.10.1, 10.10.3 to 10.10.5
    - Control 11.1.1
    - Controls 11.2.1, 11.2.2 and 11.2.4
    - Control 11.3.3
    - Control 11.4.1
    - Control 11.6.1
    - Controls 13.1.1 and 13.1.2
    - Controls 13.2.1 and 13.2.3
    - Control 15.2.1
- Phase 2:
  - PO6 (Target Maturity Level 4)
    - No associated ISO 17799 controls
  - PO7 (Target Maturity Level 4)
    - Control 10.3.2
    - Control 11.7.1
  - PO9 (Target Maturity Level 4)
    - No associated ISO 17799 controls
  - DS1 (Target Maturity Level 4)
    - No associated ISO 17799 controls
  - DS2 (Target Maturity Level 4)
    - Control 10.2.1
- Phase 3:
  - DS7 (Target Maturity Level 4)
    - No associated ISO 17799 controls
  - DS7 (Target Maturity Level 4)
    - No associated ISO 17799 controls

- DS10 (Target Maturity Level 4)
    - No associated ISO 17799 controls
- DS11 (Target Maturity Level 5)
    - Control 10.5.1
    - Control 12.2.1
- DS12 (Target Maturity Level 4)
    - No associated ISO 17799 controls

- Phase 4: The remainder of the COBIT objectives and their mapped ISO 17799 security controls.

The phases and controls of the IT-SOP, as well as their placement in the IT governance framework project, are depicted in Figure 6.6.



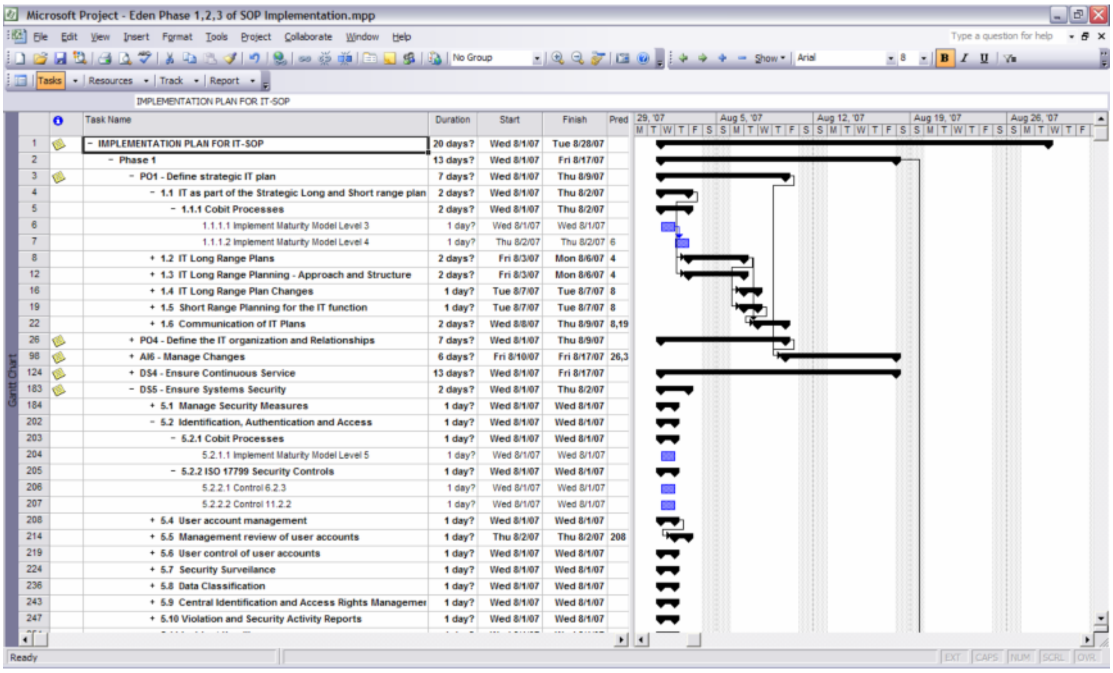
Input Factors of Influence
Municipal Legislation
Integrated Development Plan
Audit Reports (Local Mun.)
Lack of Vision and defined Standards and Guidelines
Master Systems Plan
Lack of Synchronization and Coordination
Current Situation at Eden DM
Eden (Dist. & Local) Municipal IT Problem Situation
Lack of IT Governance and Information Security Controls
Proposed Solution to Eden DM
Eden (Dist. & Local) IT Strategic Objective Plan (IT-SOP)
Sound IT Governance and Information Security Controls
IT-Strategic Objective Plan
IT Strategic Objective Implementation plan
IT-SOP Phase 1
COBIT Processes: PO1, PO4, AI6, DS4 & DS5 Plus mapped ISO17799 Controls
IT-SOP Phase 2
COBIT Processes: PO6, PO7, PO9, DS1 & DS2 Plus mapped ISO17799 Controls
IT-SOP Phase 3
COBIT Processes: DS7, DS8, DS10, DS11 & DS12 Plus mapped ISO17799 Controls
IT-SOP Phase 4
COBIT Processes: Rest of COBIT processes Plus mapped ISO17799 Controls

Figure 6.6: The IT-SOP

The most important aspect of the IT-SOP is that it is regarded as a continuous, ongoing effort towards implementing sound IT governance practices. Therefore, the implementation efforts should be integrated into the overall municipal culture of corporate governance. To initiate this process, an extensive project plan was defined for the IT-SOP.

This project plan was developed as part of the IT governance framework project to assist the municipalities with the task of implementing the IT-SOP. As stated in the previous section, the IT-SOP consists of four phases, and that it is the responsibility of the municipality to define time frames, budgeting and the allocation of resources to the project. The project plan was developed using Microsoft's Office Project 2003 tool.

The project was structured in a hierarchy consisting of the overall project as the highest entity, with the four phases as its subordinates. This hierarchy structure breaks the project into smaller, more manageable project components. An advantage of managing the project in this way is that it is only required to assign a time frame to each objective and ISO 17799 control. These durations all add together to provide the overall time required for the objective to be implemented, and the time required for each objective provides the time required for the phase to be completed, and so forth. Another advantage of using the project plan in such a way is that the municipality can now pursue the further implementation of the IT-SOP, i.e., define additional phases from the remaining COBIT objectives, time frames, task dependencies, etc., in the same project plan. The advantages of a project management approach have already been mentioned in Chapter 4. An extract of the project plan hierarchy is depicted in Figure 6.7 and the full project plan is available as Appendix G, attached to this dissertation.


Microsoft Project - Eden Phase 1,2,3 of SOP Implementation.mpp
File Edit View Insert Format Tools Project Collaborate Window Help
Type a question for help
No Group
Show
Arial
8
Tasks Resources Track Report
IMPLEMENTATION PLAN FOR IT-SOP
Gantt Chart
29, '07
Aug 5, '07
Aug 12, '07
Aug 19, '07
Aug 26, '07
Ready
EXT CAPS NUM SCRL OVR

		Task Name	Duration	Start	Finish	Pred
1		− IMPLEMENTATION PLAN FOR IT-SOP	20 days?	Wed 8/1/07	Tue 8/28/07	
2		− Phase 1	13 days?	Wed 8/1/07	Fri 8/17/07	
3		− PO1 - Define strategic IT plan	7 days?	Wed 8/1/07	Thu 8/9/07	
4		− 1.1 IT as part of the Strategic Long and Short range plan	2 days?	Wed 8/1/07	Thu 8/2/07	
5		− 1.1.1 Cobit Processes	2 days?	Wed 8/1/07	Thu 8/2/07	
6		1.1.1.1 Implement Maturity Model Level 3	1 day?	Wed 8/1/07	Wed 8/1/07	
7		1.1.1.2 Implement Maturity Model Level 4	1 day?	Thu 8/2/07	Thu 8/2/07	6
8		+ 1.2 IT Long Range Plans	2 days?	Fri 8/3/07	Mon 8/6/07	4
12		+ 1.3 IT Long Range Planning - Approach and Structure	2 days?	Fri 8/3/07	Mon 8/6/07	4
16		+ 1.4 IT Long Range Plan Changes	1 day?	Tue 8/7/07	Tue 8/7/07	8
19		+ 1.5 Short Range Planning for the IT function	1 day?	Tue 8/7/07	Tue 8/7/07	8
22		+ 1.6 Communication of IT Plans	2 days?	Wed 8/8/07	Thu 8/9/07	8,19
26		+ PO4 - Define the IT organization and Relationships	7 days?	Wed 8/1/07	Thu 8/9/07	
98		+ AI6 - Manage Changes	6 days?	Fri 8/10/07	Fri 8/17/07	26,3
124		+ DS4 - Ensure Continuous Service	13 days?	Wed 8/1/07	Fri 8/17/07	
183		− DS5 - Ensure Systems Security	2 days?	Wed 8/1/07	Thu 8/2/07	
184		+ 5.1 Manage Security Measures	1 day?	Wed 8/1/07	Wed 8/1/07	
202		− 5.2 Identification, Authentication and Access	1 day?	Wed 8/1/07	Wed 8/1/07	
203		− 5.2.1 Cobit Processes	1 day?	Wed 8/1/07	Wed 8/1/07	
204		5.2.1.1 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07	
205		− 5.2.2 ISO 17799 Security Controls	1 day?	Wed 8/1/07	Wed 8/1/07	
206		5.2.2.1 Control 6.2.3	1 day?	Wed 8/1/07	Wed 8/1/07	
207		5.2.2.2 Control 11.2.2	1 day?	Wed 8/1/07	Wed 8/1/07	
208		+ 5.4 User account management	1 day?	Wed 8/1/07	Wed 8/1/07	
214		+ 5.5 Management review of user accounts	1 day?	Thu 8/2/07	Thu 8/2/07	208
219		+ 5.6 User control of user accounts	1 day?	Wed 8/1/07	Wed 8/1/07	
224		+ 5.7 Security Surveilance	1 day?	Wed 8/1/07	Wed 8/1/07	
236		+ 5.8 Data Classification	1 day?	Wed 8/1/07	Wed 8/1/07	
243		+ 5.9 Central Identification and Access Rights Managemer	1 day?	Wed 8/1/07	Wed 8/1/07	
247		+ 5.10 Violation and Security Activity Reports	1 day?	Wed 8/1/07	Wed 8/1/07	

Figure 6.7: Project Plan for the Implementation of the IT-SOP

Implementing a project management approach would ensure that the COBIT objectives and the ISO 17799 controls are implemented in an efficient manner, using the least amount of time and resources. The project also required that project results, such as the target maturity levels, etc., be reported at various stages in the research project's progress.

The IT-SOP was presented to the district municipality during the final stages of the IT-SOP project. The executive summary of the IT-SOP, as well as an excerpt of the IT-SOP is available as Appendix E and F, but due to its extensive size of more than 100 pages, the full IT-SOP was not attached. During this presentation, the executive management, municipal mayor, manager and IT management were present. The municipality's executive management then proposed the IT-SOP to the municipal council where it was subsequently accepted and recognised as a best practice for the municipality.

6.4 Conclusion

The IT-SOP was compiled from the results obtained from the case studies conducted at the district and the underlying local municipalities. Various research tools had to be developed to obtain the required results. These tools included the COBIT and ISO 17799 gap analysis tools, as well as the questionnaires to gather all the data before inputting it into the gap analysis tools. The IT-SOP is made up of four phases, of which the first three phases contain between four and six COBIT objectives. These three phases contain the mandatory COBIT objectives which must be implemented by the district and local municipalities. After the implementation of phase 3, it is then the responsibility of the municipality to define additional phases and select the desired COBIT objectives from the provided list. Each COBIT objective contains its mapped ISO 17799 security controls, as well as performance measurement metrics and factors which will ensure the success of the objective. To facilitate the implementation of the IT-SOP by the municipality, a project plan was produced which graphically depicts the IT-SOP as a series of project tasks and milestones.

At various stages in the IT governance framework project, feedback, project progress and results were presented to the district and local municipalities. These reports were produced during the initial phases of the project to provide information, after the case studies to report on compliance performance, as well as at the end of the project to provide the required guidance, strategy and tools required to successfully implement the IT-SOP in the district municipality and its underlying, local municipalities.

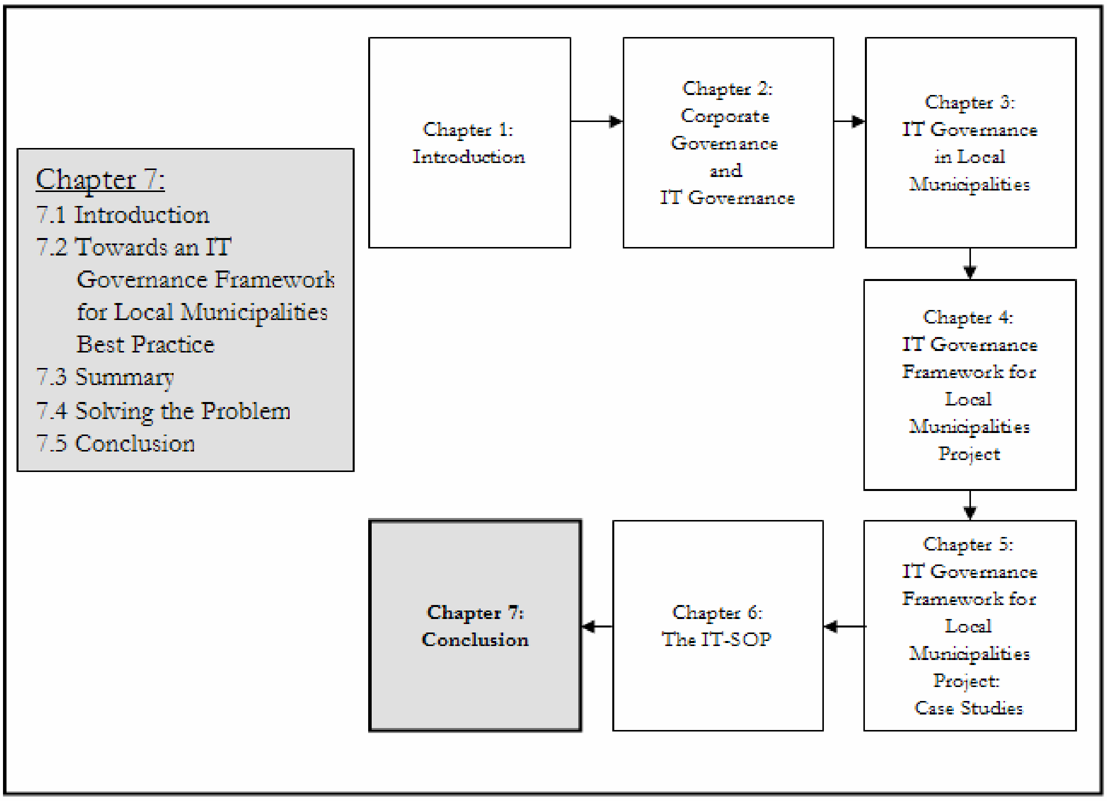
It is currently the responsibility of the municipalities to allocate resources and to implement the IT-SOP; therefore, the next and final chapter will provide an overview of the project, what has been done, what factors proved to be influential in this project, as well as what future work can be expected, based on the outcomes of this project.

Part IV

Conclusion

Chapter 7

Conclusion


Chapter 7:
7.1 Introduction
7.2 Towards an IT Governance Framework for Local Municipalities Best Practice
7.3 Summary
7.4 Solving the Problem
7.5 Conclusion
Chapter 1: Introduction
Chapter 2: Corporate Governance and IT Governance
Chapter 3: IT Governance in Local Municipalities
Chapter 4: IT Governance Framework for Local Municipalities Project
Chapter 5: IT Governance Framework for Local Municipalities Project: Case Studies
Chapter 6: The IT-SOP
Chapter 7: Conclusion

Chapter 7 – Conclusion

7.1 Introduction

Sound IT governance and corporate governance are both critical for the well-being of any municipality. Therefore, the IT function, IT infrastructure and the systems that guard the electronic information assets should be adequately protected and governed. This dissertation aims to introduce an IT governance framework that is based on the international accepted best practice, COBIT and the ISO 17799 standard for information security management. Furthermore, this framework has been tailored to suit the auditing and operational requirements of municipalities. The process of creating this framework is discussed in detail in the chapters of this dissertation.

Several key topics were discussed through the various chapters in this dissertation to position this framework within the municipal governance sphere. Some of these topics include corporate governance in general, IT governance and the requirements and current problems of IT currently in local governments. Executive municipal management should be aware of the responsibility to adequately protect and govern the information assets, whereas IT governance is no longer a more technology issue that has to be dealt with by a specific organisational department. Sound IT governance, as part of overall corporate governance, is only possible when a pro-active approach towards effective IT governance is initiated by the board. This approach will ensure that the IT infrastructure and systems are eventually aligned to the municipal mission, vision and objectives. The IT investment can only then deliver the envisioned benefits and value to the municipality. The proposed framework, when successfully implemented by a municipality, should enable the municipality to properly position the IT function within the overall organisational structure, ensure board-level representation or a strategic oversight committee for IT and ensure that IT is supportive of the overall municipal objective strategies.

7.2 Towards a Best Practice for IT Governance in Local Municipalities

The development of the IT-SOP was aimed at the IT governance requirements for a specific district and its local underlying municipalities. However, there are three main reasons why the IT-SOP, with a few amendments through future research, should be applicable to most, if not all, South African municipalities. The reasons for this are briefly discussed in the next few paragraphs.

The first reason why the IT-SOP should be applicable to any municipality is that municipalities typically uses computers and systems to store, process and communicate information to internal or external recipients. Thus, the IT-SOP is applicable to any municipality that uses IT to store, process and communicate information.

The municipal IDP and MSP plans are the second reason why the IT-SOP should be applicable to any municipality. Legislative mandates, such as the Municipal Systems Act (No. 32 of 2000) and the Municipal Structures Act, require that every municipality should submit its IDP and MSP plans to government. The IT-SOP fits between the IDP and the MSP, ensuring the alignment of the MSP with the IDP. Thus, the IT-SOP is applicable to any municipality.

The annual municipal IT audits report are the third reason why the IT-SOP should be applicable to any municipality. To briefly review, an annual IT audit is conducted before the financial information of a municipality is audited to ensure the integrity of the internal controls. These reports highlight any shortcomings that must be mitigated, as measured against certain objectives from the COBIT framework. The IT-SOP surpasses all of the IT audit requirements and therefore enables the municipality not only to comply with audit regulations, but to base its IT operations on a solid IT governance practices' foundation.

During the project's literature survey, many IT governance-related issues were identified through media reports. These issues were highlighted, and additional issues that were identified during this project were discussed. The IT departments are limited in various ways from efficiently governing their IT infrastructure and related systems. Some media reports, which reported on the results of research on municipalities' IT departments, indicated that there are many problems currently with IT within municipalities. Chapter 3 discussed these reported problems in detail. For review purposes, these problems included the following:

- The IT departments are not ideally placed within the corporate hierarchies;
- The budgets for the IT department are not ideal;
- There is a shortage of the necessary skills;
- There is a shortage of human resources;
- There is a lack of understanding of the IT sector and its policies.

During the course of the project, various additional factors and constraints were identified as limiting IT governance efforts in a municipality. These problems, although not published in media articles, were identified by the IT management function of the different municipalities. Taking into account these limitations, various recommendations, based on COBIT, were made to the municipalities. These additional limiting factors, constraints and recommendations are:

- Very little strategic IT planning is aligned with the long-term goals of the municipality;
- There is a lack of full, formally defined and documented operating procedures;
- The IT function is not ideally positioned within the organisational structure;
- The importance and risks regarding IT are not recognised nor understood by management;
- There is seemingly a lack of dedicated management commitment via an oversight or steering committee;
- There are budget limitations regarding IT development. At the COGITRIS 2007 conference, a municipal delegate revealed that, keeping the importance of IT in mind, the IT function of his municipality receives a mere 1.5% of the total budget and both human resources and development have to be financed from this as well. (Personal communication, 2007);
- Ineffective, slow or hesitant decision-making due to systems not functioning properly;
- There are unclear reporting line protocols between the IT function and executive management;
- There are IT-skills shortages;
- There is a lack of human resources in the IT function.

All of the above factors contributed towards the lack of proper IT governance practices and procedures within local municipalities. Lack of proper, published guidelines, collaboration and coordinated efforts result in many municipalities implementing IT systems and management procedures as they see fit, which results in many disparate information islands, since many of the systems which are used within municipalities, as well as between different municipalities, are not compatible. Thus, the compiling of business-critical, strategic information has become an enormous task which is often very time-consuming, and results in delayed information.

Therefore, it also became a requirement of the IT governance project to define an IT governance framework which would assist municipalities to define strategic collaborative processes and coordinated procedures enabling them to have coordinated IT governance processes. There are many advantages to having a coordinated effort in bringing about sound IT governance within a district. Some of these envisioned advantages for the municipalities were:

- Certain municipalities could provide IT-related functions as a service to other municipalities within the district which are unable to perform those functions. Examples include information hosting, storage of backups, disaster-recovery sites, etc. This strategy is in line with the government's view of a shared-services model between municipalities and governments.
- Possible similar systems within municipalities of the same district. This will allow them to gather and consolidate information much faster and efficiently and with fewer errors.

7.3 Summary

Chapter 1 presented the subject area of the study, stated the primary research questions and then introduced the areas of corporate governance and IT governance and how they apply to local municipalities. It was noted how little IT strategic planning is taking place within local governments, and that the possible cause thereof might be that there are very few published standards or guidelines for IT governance within local municipalities. These arguments form the basis around which this study was conducted. These arguments support the main objective of this project, which was to develop and present a framework for the effective governance of IT within a municipality. Additional objectives were also defined for this project to ultimately achieve the main objective. These additional objectives were to investigate which COBIT objectives and ISO 17799 controls are applicable to municipalities and to what extent do these objectives and controls have to be implemented.

Corporate governance and IT governance were the topics of **Chapter 2**. An overview was presented on corporate governance and it was explained what is meant by good corporate governance. It was noted that possibly the biggest contributor to poor corporate governance is the lack of protection and the governance of the information assets, possibly the most valuable organisational assets. Examples of major organisational failures that were the result of poor corporate governance were highlighted. The value of information and the organisational information assets were then discussed. It was noted that an organisation's risk of failure due to bad governance is reduced if it has an effective IT infrastructure and systems in place, as well as a sound governance structure to govern these. IT governance was then discussed. COBIT was presented as the IT governance framework, developed by ISACA, and published by the IT Governance Institute (ITGI). It was noted that IT systems are no longer only a "nice-to-have" anymore, but are an important foundation on which to base any organisation's business processes. It was further explained how IT governance aims to support corporate governance by protecting the information assets and to align the IT infrastructure strategy to the organisational, business strategy in order for IT to support the organisation.

The lack of good IT governance in local governments or municipalities was discussed in **Chapter 3**. The scope of corporate and IT governance was narrowed down to district and local governments. Various statistics were presented which were the results of previous research by a third-party research company. The problem area was discussed in detail and the shortcomings highlighted. The concept of an IT governance framework for local municipalities, how this framework should cater for the requirements of the municipal IDP and MSP plans and how it should be based on international best practices and standards was then introduced. The COBIT best practice and the ISO 17799 standard were then presented and discussed in detail. The links between these two resources and the advantages thereof were also highlighted.

Chapter 4 outlined the IT governance framework project that forms part of the bigger project, of which this dissertation is the main deliverable. The factors, such as the IDP and MSP, lack of guidelines, the audit reports and the municipal legislation were discussed. Next, the implementation of IT governance frameworks was discussed, followed by Poole's implementation methodology and Kordel's methodology. The framework implementation steps of both Poole and Kordel were discussed, as well as how these two methodologies were combined to produce the methodology that was employed for the IT-SOP project. From this combined methodology, various theoretical project phases and steps were defined, after which they were then applied to the IT-SOP project and discussed in the project anatomy. The project outcomes and deliverables were then outlined and discussed, after which an in-depth description of the annual IT audit reports was provided.

The case studies and their results were discussed in **Chapter 5**. The gap analysis layout and the information gathering objectives were defined. The information to be determined was which COBIT objectives were applicable to a municipality, what the target maturity levels of the identified objectives were and what the current level of implementation was. It was noted that the target maturity level for each objective was determined by evaluating the audit report requirements, as well as the opinions from IT management that were gathered during the interview sessions. The gap analysis evaluation tool, designed specifically for the case studies, was introduced and the model for the scoring and the case study results was discussed. Further, the consolidation of the case study results was discussed and the final maturity models for each of the identified COBIT objectives were provided. These final maturity levels provided the basis on which the IT-SOP was defined. The case studies determined that all of the COBIT objectives are relevant to a municipality and that not all of the objectives should be implemented at the optimal maturity level (level 5). Further, the ISO 17799 information security standard was discussed and the outline of the standard was provided. The relationship between COBIT and ISO 17799 was highlighted and the mapping between these two references, as well how they complement each other, was discussed.

Chapter 6 discussed the IT-SOP, the main deliverable for this IT governance framework project. The process regarding the development of the IT-SOP was discussed, as well as the flow of the project and the research methods that contributed the required information to it. This chapter discussed the initial investigation of and municipal proposal for the IT-SOP project, the COBIT case studies and the COBIT gap analysis tool that was designed specifically for the task. Various examples of the tool as well as appendices were provided in this chapter. Further, the determining of the relevant ISO 17799 information security controls were discussed and the tool that was designed for this task was highlighted as well. The process of mapping the COBIT objectives to the ISO 17799 controls was then also discussed. The objectives of the IT-SOP, as well as its implementation phases, COBIT objectives, associated ISO 17799 controls and project plan were discussed in detail. It was noted that the IT-SOP was presented to the district municipality's council where it was accepted and recognised as a best practice for the district municipality and its underlying local municipalities.

This project was presented at conferences such as the "Afrikaanse Akademie vir Wetenskap en Kuns 2006", LogICT 2006, COGITRIS II 2007 and SAICSIT 2007.

Papers were submitted to these conferences, as well as posters that were created for display purposes. For more information on these outputs, see Appendix H.

The various chapters of this study helped to support the main objective. It is, however, important to understand how this was accomplished and how the primary research question was resolved.

7.4 Solving the Problem

The primary research question of this dissertation was: "How can COBIT be tailored into a best practice IT governance framework to suit the requirements of local municipalities in South Africa that will ensure that the IT infrastructure and systems are aligned with the municipal objectives, provide sufficient risk and threat mitigation and enable local governments to coordinate and collaborate on strategic planning and overall IT governance?". This question helped state the primary research objective of the study, which was to draft a best practice framework to effectively mitigate Information Technology-related risks in local governments and to provide an effective service to both internally-related governance issues and externally-related service delivery. A number of secondary objectives were defined to help accomplish the primary objective of this project and to provide a resolution to the problem statement.

The first of these secondary objectives was to develop a base framework that contains the COBIT objectives that are applicable to a municipality. The dissertation achieved this objective by performing five steps towards the development of the IT-SOP. The first step was to conduct various case studies at a district municipality and its local, underlying municipalities. The case studies, combined with questionnaires, interviews and the study of the annual IT audit reports were required to accurately determine which COBIT objectives were applicable to a local municipality. The conclusion from these case studies was that all of the COBIT high-level objectives are applicable to a local municipality.

The second of these five steps was to determine the current maturity levels for each of the identified COBIT high-level objectives. The dissertation achieves this objective by discussing the various COBIT gap analyses that were performed at the various local municipalities and the district municipality, as part of the case studies. A tool was required to conduct each gap analysis, since the tools available on the market was either too extensive and expensive, or they were not able to provide the applicability, current and target maturity levels for the COBIT objectives. Therefore, a tool was designed and produced as part of this dissertation to provide this information. The maturity level for a high-level COBIT objective could be determined by measuring the current maturity level for each detail control objectives that form part of the high-level objectives against the maturity model of the objective. These maturity levels were determined by conducting interviews and investigating the audit report findings. The average of the detailed control objectives' maturity levels provided an indication as to the current maturity level of the high-level control objectives.

To identify the target maturity level for each identified COBIT high-level objective was the third step. Various COBIT case studies, questionnaires and interviews were conducted in the district and local municipalities in order to meet this objective. Each identified COBIT objective was discussed and the target maturity level was determined through interviews, as well as investigating the auditing requirements from the annual, municipal IT audit reports, where available, as only some of the COBIT high-level objectives had been investigated during an audit and stated in the audit report. The target maturity levels of the identified COBIT objectives were then combined to form the foundation of the IT-SOP.

The fourth step was to determine which of the identified COBIT high-level objectives that must be improved are at a higher priority than the rest. This objective was met through examining the results from the case studies, discussing the various IT audit reports and how they played a role in determining which of the audit findings and identified improvements have a critical, high or medium risk level, as stated in the audit reports. These risk levels, as well as interviews that were conducted to determine the improvement strategy, made it possible to prioritize all of the identified COBIT objectives. The findings were that there were certain COBIT objectives that were more important than others and that these objectives had to be implemented or improved earlier than the rest. The identified COBIT objectives were then grouped, according to their importance, into various implementation phases, containing between four and six objectives per phase. The higher-priority objectives were included in the first phase. Phase 1 of the IT-SOP implementation contains the most important COBIT objectives, namely PO1, PO4, AI6, DS4 and DS5.

The last step was to determine how the ISO 17799 information security standard can be used in conjunction with COBIT in order to complement the proposed IT governance framework for local municipalities. For this purpose, the ISO 17799 information security standard was discussed in detail. Further, its relationship with COBIT was investigated by discussing the available mapping literature that explains, in detail, how the ISO 17799 controls are related to the various COBIT objectives. The advantages of using the high-level, general, IT-governance COBIT framework were discussed and it was noted that there were many reasons why COBIT and ISO 17799 complement each other and could be implemented together. The detailed, issue-specific ISO 17799 standard in synergy with COBIT were also discussed. By completing these five required steps, it can be concluded that the first secondary objective was met satisfactory.

The second secondary objective was to combine the ISO 17799 security controls to the identified COBIT objectives. An ISO 17799 analysis was conducted at the district municipality to determine which of the ISO 17799 controls were applicable to a municipality. The tool that was developed for this purpose was also discussed. During this analysis, information was gathered on which ISO 17799 controls are applicable to a municipality, which of these identified controls are not implemented at all, which are partially implemented to the ISO 17799 specification and require further improvement and which are fully implemented to the ISO 17799 specification. It was found that certain ISO 17799 controls were not applicable to a municipality and that these controls could be ignored. Only the controls that were applicable and not implemented, or partially implemented, were selected for the base framework. The controls were then integrated with their associated COBIT objectives and any redundant mappings of the same ISO 17799 information security control to other COBIT objectives in subsequent phases were eliminated, since an ISO 17799 control is only required to be implemented once for it to exist. Therefore, it can be accepted that this secondary objective was accomplished successfully.

The third and last of the secondary objectives of this dissertation was to develop a project plan for the IT-SOP. This project plan would initiate and facilitate the implementation of the IT-SOP in the municipality. The project plan was developed by creating tasks for all of the COBIT detailed control objectives and ISO 17799 information security controls as part of the hierarchical structure of the project plan, which reflects the hierarchy of the IT-SOP. This project plan met the requirements of the last secondary objective and therefore, this secondary objective has been met.

All of the secondary objectives has been met and it can be concluded that the primary objective was also successfully met, since the base COBIT objectives framework, the mapped ISO 17799 security controls and the project plan constitute the IT governance framework (the IT strategic objective plan) for local municipalities.

7.5 Conclusion

Information is a very important asset to any organisation, including municipalities, and is considered the life-blood of the organisation. Therefore, information should be effectively managed to ensure that it is readily available, but protected against threats to compromise the integrity and confidentiality thereof. Since most of an organisation's information is stored on and communicated through computer systems and networks, it is of critical importance that the IT systems should be adequately governed. The proposed IT governance framework for local municipalities, the IT-SOP, helps a municipality to develop procedures and processes that are modelled on the IT-SOP. The IT-SOP was developed using applicable COBIT objectives and their associated ISO 17799 controls. These two industry codes of practice help to address most aspects of IT-related risks in a municipal environment. The IT-SOP has also been recognised and accepted by the district municipality as a best practice for IT governance in the region. Further research would involve the defining of the IT-SOP on a generic model that caters for the IT-governance requirements from most South African municipalities. Functionality would also have to be added for a specific municipality to recognize its relevant improvement opportunities from both COBIT and ISO 17799 and to incorporate them in the municipality's overall IT-governance implementation strategy. Nonetheless, implementing IT-governance is an ongoing journey and not a destination, requiring ongoing improvements and changes to keep up with new technologies and an ever-evolving environment. Further research on this research topic is envisaged towards expanding this IT governance framework to all South African local municipalities. This research will enable the measurement of the success of implementing the proposed IT governance framework in local municipalities.

References

17799.com. (2006). *ISO 17799:2000 and ISO 17799:2005 Mapping of security categories between 2000:2005*. Available from URL: http://www.17799.com/papers/2000v2005.xls. Cited on 26 July 2006.

Allen, Julia H. (2006). *How much security is enough?* Available from URL: https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/management/566.html. Cited on 7 August 2007.

Botha M, von Solms, R. (2001). *The utilization of trend analysis in the effective monitoring of information security*. Information Management & Computer Security. Volume 9. Number 5. 2001. Pages 237 – 242.

Cadbury, A. (1992). *The Financial Aspects of Corporate Governance*. The report of the Cadbury Committee on The Financial Aspects of Corporate Governance: The Code of Best Practice. Corporate Governance: An International Review 1 (3), page 124.

Cantor, M. Sanders, J.D. (2007). *Operational IT Governance*. Available from URL: http://www.ibm.com/developerworks/rational/library/may07/cantor_sanders/index.html. Cited on 3 August 2007.

Centre for Business Research. (2004). *Project: Cooperation, Stakeholder Representation and Business Performance*. Available from URL: http://www.cbr.cam.ac.uk/research/programme2/project2-1.htm. Cited on 16 March 2007.

Changepoint Corporation. (2004). IT *Governance: The Board's – and the CIO's – Business.* Available from URL: http://www.compuware.com/media.asp?cid=701000000004etf. Cited on 26 April 2006.

Cliffe Dekker. (2002a). *King report on corporate governance for South Africe 2002 – What it means for you*. Available from URL: http://www.cliffedekker.co.za/literature/corpgov/compenforce.htm. Cited on 28 June 2006.

Cliffe Dekker. (2002b). *King report on corporate governance for South Africe 2002 – What it means for you.* Available from URL: http://www.cliffedekker.co.za/literature/corpgov/ directors.htm. Cited on 28 June 2006.

CompassPoint, (2006). *Strategic Planning, Long-Range planning and Operational Planning.* Available from URL: http://compasspoint.org/askgenie/printAll.php?tpid=12 Cited on 27 September 2007.

CPA Audit (2007). *Corporate Governance.* Available from URL: http://www.cpaaudit.co.uk /pages/corpgovernance.html. Cited on 27 September 2007.

ECT Act. (2002). *Electronic Communications and Transactions Act, nr 25 of 2002.* Available online from URL: http://www.acts.co.za/ect_act/index.htm. Cited on 16 March 2007.

Ernst and Young. (2004). *Developments in Corporate Governance since King II Report.* Available from URL: http://www.ey.com/global/content.nsf/South_Africa/08_Nov_04_ Developments_in_Corporate_Governance_since_King_II_Report. Cited on 1 March 2006.

Gamma. (2007). *Corporate Governance: So what's the problem?* Available from URL: http:// www.gammassl.co.uk/bs7799/corporate%20governance/index.html. Cited on 20 August 2007.

George Municipality. (2006). *George Municipality IT Audit Report for 2006.* George Municipality.

Global Union Research Network (GURN). (2006). *Topic: Corporate Governance.* Available from URL: http://www.gurn.info/topic/corpgov/index.html. Cited on 9 November 2006.

Government Gazette. (2000). *Municipal Systems Act, number 32 of 2000.* Government Gazette Newspaper. Volume 425. Number 21776.

Government Gazette. (1998). *Municipal Structures Act, number 117 of 1998.* Government Gazette Newspaper. Volume 402. Number 19614.

IMFO. (2003). *Local Government: Municipal Finance Management Act, number 56 of 2003.* Available from URL: http://www.info.gov.za/gazette/**act**s/2003/a56-03.pdf Cited on 11 June 2006.

IT Governance Institute. (2000a). *About IT Governance : Objectives of IT Governance.* Available from URL: http://www.itgi.org/template_ITGI.cfm?Section=Objectives &Template=/ContentManagement/HTMLDisplay.cfm&ContentID=19661 Cited on 18 April 2007.

IT Governance Institute. (2007a). *Board Briefing on IT Governance, 2nd Edition.* Pages 11, 37. Available from URL: http://www.itgi.org/ Cited on 7 October 2007.

IT Governance Institute (ITGI). (2000b). *Cobit Student Book.* Page 7.

IT Governance. (2007b). *COBIT – Control Objectives for Information and Related Technology.* Available from URL: http://www.itgovernance.co.uk/cobit.aspx Cited on 7 October 2007.

IT Governance Institute. (2004). *COBIT Mapping: Mapping ISO/IEC 17799:2000 to COBIT.* Available from URL: http://www.itgi.org/ Cited on 17 April 2007.

Keen, P. G. W. (1991). *Shaping the future: Business design through information technology.* Cambridge: Harvard Business School Press.

King Report. (2002). *The King Report on Corporate Governance for South Africa.* Available from URL: http://www.iodsa.co.za/IoD%20Draft%20King%20Report.pdf. Cited on 16 April 2006.

Kordel, L. (2004). *IT Governance Hands-on: Using COBIT to Implement IT Governance.* Information Systems Control Journal, Volume 2, 2004. Published by: Information Systems Audit and Control Commission. Page number unspecified.

KPMG. (2004). *Creating Stakeholder value in the information age.* Available from URL: http://196.30.226.221/office/kpmg/0412020933.htm. Cited on 20 April 2007.

Kurkure, AP. (2006). *Corporate Governance.* Available from URL: http:// 2006.confex.com/uicc/uicc/techprogram/P10186.HTM. Cited on 23 August 2007.

Loyd, S. (2004). *Corporate Governance and Information Security.* Available from URL: http://www.sans.org/reading_room/whitepapers/casestudies/1382.php?portal=1fc15b56f31b6c512a3c66c51d845041. Cited on 23 August 2007.

Marchewka, J. (2003). *Information Technology Project Management.* Pages 4 – 6. Published by: John Wiley & Sons. ISBN: 0-471-39203-0.

McCue, A. (2007). *Poor IT Governance key to project failures.* Available from URL: http://news.zdnet.co.uk/itmanagement/0,1000000308,39286542,00.htm?r=5. Cited on 13 July 2007.

McKinsey Quarterly. (2007). *Three surveys on corporate governance.* Available from URL: http://www.mckinseyquarterly.com/Governance/Boards/Three_surveys_on_corporate_governance_965_abstract. Cited on 27 September 2007.

Mochiko, T. (2005a). *Information Technology baffles most municipalities.* Available from URL: http://www.busrep.co.za/index.php?fArticleId=2454865&fSectionId=612&fSetId=304. Cited on 13 March 2006.

Mochiko, T. (2005b). *Municipalities must develop ICT infrastructure.* Available from URL: http://www.busrep.co.za/index.php?fSectionId=561&fArticleId=2878906. Cited on 13 March 2006.

Mossel Bay Municipality. (2006). *IT Audit report for the Mossel Bay municipality*. Mossel Bay Municipality.

Oasis. (2002). *Oasis*. Available from URL: http://ssdoo.gsfc.nasa.gov/nost/isoas/presentations/USDA19990219/tsld013.htm. Cited on 27 March 2006.

Perry, J. T., Schneider, G. P. (2001). *Electronic commerce*. In (Second ed., pp. 193 – 236). Course Technology.

Poole, V. (2007). *A Governance Framework*. Available from URL: http://www.nccmembership.co.uk/pooled/articles/BF_WEBART/view.asp?Q=BF_WEBART_195169. Cited on 16 August 2007.

Queensland Government. (2002). *Corporate Governance*. Available from URL: http://education.qld.gov.au/strategic/policy/guidelines/risk/corporate.html. Cited on 16 August 2007.

Ramaswamy, V. (2005). *Corporate Governance and the Forensic Accountant*. CPA Journal. March 2005 issue. Available from URL: http://www.nysscpa.org/cpajournal/2005/305/essentials/p68.htm. Cited on 15 August 2007.

Ryan, C. (2007). *Corporate Governance is about collaboration, not annual reports*. Available from URL: http://www.btimes.co.za/top100/t29.htm. Cited on 23 June 2007.

Standards South Africa. (2005a). *ISO/IEC 17799 Code of practice for information security management*. Publisher: Standards South Africa, Pages x to 6.

Standards South Africa, (2005b). *ISO/IEC 17799: Code of practice for information security management*. Available from URL: http://www.standardssouthafrica.org.za. Cited on 10 June 2007.

South African Government Information. (1996). *Constitution of South Africa.* Chapter 7, section 153. Available from URL: http://www.info.gov.za/documents/constitution/1996/96cons7.htm Cited on 12 August 2007.

Tarimo, J. (2006). *Corruption linked to poor corporate governance.* Available from URL: http://www.ipp.co.tz/ipp/guardian/2006/04/05/63599.html. Cited on 7 September 2006.

Thompson K, von Solms R. (2005). *Information Security Obedience: a definition.* Computers and Security. Volume 24. Issue 1. February 2005. Pages 69 – 75.

Thomson, K. (2003). *Integrating information security into corporate culture.* Unpublished. Masters dissertation, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa.

Von Solms, B. (2005). *Information Security governance: COBIT or ISO 17799 or both?* Computers and Security. Volume 24. Issue 2. Pages 99 – 104.

Wu, S. (2007). *Identifying, Disseminating, and Implementing Best Practices.* RAND Corporation. Available from URL: http://www.vc.wisc.edu/apr/T+R/BestPracticesSeminar.pdf Cited on 17 October 2007.

Part V

Appendices

Appendix A

COBIT Gap Analysis Questionnaire

Introduction

For an organisation to be well governed, its governance practices have to be based on tried and tested methods, or best practices. There are many governance best practices and frameworks available, focusing on different aspects of organisational governance, such as Financial and Information Technology governance.

CobiT is a governance framework that is focused on Information Technology and is short for Control Objectives for Information and related Technology and was developed by the IT Governance Institute (ITGI). It is a very well accepted, international Best Practice. It is used to optimize the use of IT, as well as aligning IT with the strategic objectives and overall goals of the organisation.

The CobiT framework contains 4 domains spanning the overall IT process and function within an organisation. Within these 4 domains are 34 high-level control objectives, with each objective having more detailed objectives and practices, targeting specific IT functions.

Management guidelines are also provided by CobiT that contain tools to measure the organisation's IT infrastructure against these 34 objectives. These tools include Critical Success Factors, Key Goal Indicators and Maturity Models.

Organisations need timely, accurate and appropriate information to satisfy its information requirements. CobiT provides these measures to make sure that information satisfies these criteria.

Purpose of this questionnaire

The purpose of this questionnaire is to identify the 'gap' between the current state of Information Technology governance in the organisation at current and the requirements of the CobiT governance standard regarding Information Technology.

The questionnaire contains questions regarding the 4 overall IT domains, specifically targeted towards the 34 high-level control objectives, spanning the IT organisational function. The gap between the CobiT requirements and the current state of IT governance will be calculated using the CobiT maturity model approach. A maturity model evaluates and grades each IT process in the organisation against CobiT requirements from 0 (nonexistent) to 5 (optimized).

Outcome and results

The result of this questionnaire will aid current research in the field of IT governance at local government level in order to develop a best practice, containing models and frameworks to maximize the potential and benefit that IT holds for the organisation.

Answering of questions:

Each response to the following questions should be based on the generic scale below:

0 Non-Existent	. Complete lack of any recognisable processes. The organisation has not even recognised that there is an issue to be addressed.
1 Initial.	There is evidence that the organisation has recognised that the issues exist and need to be addressed. There are however no standardised processes but instead there are ad hoc approaches that tend to be applied on an individual or case by case basis. The overall approach to management is disorganised.
2 Repeatable	Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and therefore errors are likely.
3 Defined.	Procedures have been standardised and documented, and communicated through training. It is however left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.
4 Managed.	It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
5 Optimised.	Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modelling with other organisations. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

CobiT Domain: Planning and Organizing (PO)

Business Process:	(PO1) Define a strategic IT plan						
Business Need:	Strike balance between technology opportunities and IT business requirements						
#	**Questions**	**Response**					
1.1	Long-term plans, supporting the organization’s overall missions and goals, are regularly developed by the designated authority as well as from input from information owners as well as input from internal and external stakeholders	0	1	2	3	4	5
1.2	A structured approach exists for long-term IT planning. It takes into account risk assessment results and results in a high-quality plan	0	1	2	3	4	5
1.3	How effective are change control mechanisms and policies in order to modify or update the long-term plan in a timely and effective manner?	0	1	2	3	4	5
1.4	The long-term IT plan is regularly translated into short-term IT plans that support the goals of the long-term plan. Short-term plans are regularly evaluated and modified in order to fully complement the long-term plan	0	1	2	3	4	5
1.5	IT plans are communicated to relevant organization parties in timely intervals	0	1	2	3	4	5
1.6	A process exists for business process owners to provide feedback on the quality and usefulness of long- and short-term IT plans. This feedback is used in future IT planning	0	1	2	3	4	5
1.7	Current information systems are evaluated in terms of automation, functionality, stability etc in order to evaluate how well the systems support the organization, before IT planning is commenced.	0	1	2	3	4	5
1.8	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(PO2) Define Information Architecture
Business Need:	Creating and maintaining business information model

#	**Questions**	**Response**					
2.1	Information is identified, captured and communicated to the relevant parties in order for them to perform their responsibilities effectively and in a timely manner. The information is also kept consistent with the needs of the organization.	0	1	2	3	4	5
2.2	A corporate 'Data dictionary' is kept with the organization's rules on information syntax. A framework is also in place to which Information can be classified or categorized, and allocated to an owner.	0	1	2	3	4	5
2.3	Security levels are implemented for each data classification above "no protection required". These levels reflect the minimum level of protection needed in order to safeguard the protected information	0	1	2	3	4	5
2.4	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(PO3) Determine technological direction
Business Need:	Take advantage of emerging technology to drive business strategy

#	**Questions**	**Response**					
3.1	IT Management regularly develops a technological infrastructure plan in accordance to the long-term and short-term IT plans. These plans take into account current system architecture, new technological developments, envisaged applications and price and performance changes. Future trends and regulatory requirements are also taken into consideration.	0	1	2	3	4	5
3.2	The infrastructure plan is regularly assessed in terms of redundancy, adequacy, effectiveness and other contingency indicators.	0	1	2	3	4	5
3.3	Hardware and software acquisition plans are in place that reflect the needs of the infrastructure plan	0	1	2	3	4	5
3.4	Technology norms are defined with regards to the infrastructure plan	0	1	2	3	4	5
3.5	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(PO4) Define IT organization and relationships						
Business Need:	To deliver the right IT services						
#	**Questions**	**Response**					
4.1	An IT planning and steering committee exists that oversee the IT function and its activities within the organization. This committee is represented by senior-, user management and the IT function.	0	1	2	3	4	5
4.2	The IT function is positioned in the overall organization structure with independent authority from other departments. A framework is also in place for the reviewing of the organizational structure in order to meet objectives and changing circumstances	0	1	2	3	4	5
4.3	Employees know their roles and responsibilities regarding the information systems. They have sufficient authority to fully accomplish these responsibilities, but no individual controls the key aspects of a transaction. Awareness campaigns are also held regularly to increase discipline and awareness.	0	1	2	3	4	5
4.4	Management assigned the responsibility of quality assurance to the members of the IT function's staff.	0	1	2	3	4	5
4.5	An information security manager is in charge of logical and physical security of the organization's information assets. A minimum of an organization-wide security function is in place.	0	1	2	3	4	5
4.6	All information assets have been appointed to owners, or custodians. These owners are responsible for the well-being of these assets.	0	1	2	3	4	5
4.7	Supervision practices are in place to ensure that the roles and responsibilities are properly executed by personnel in the IT function	0	1	2	3	4	5
4.8	Senior management has implemented division of roles and responsibilities to ensure that no individual has control over an entire critical process. Duty segregation is enforced in the following functions: Data entry, Network management, System administration, change management, systems development, security administration and security audit.	0	1	2	3	4	5
4.9	Regular staff requirement evaluations are performed to ensure that the IT function have sufficient, competent IT staff. These results are promptly acted on to ensure adequate IT staff for now and in the future. Position descriptions, describing both authority and responsibility, are established and regularly updated.	0	1	2	3	4	5
4.10	Management have identified key IT personnel of the IT function	0	1	2	3	4	5
4.11	To which extent are policies and procedures in place for controlling the activities of consultants external to the IT	0	1	2	3	4	5

	function, in order to protect the information assets of the organization?						
4.12	IT Management has undertaken necessary actions to establish and maintain optimum coordination between the IT function and other parties inside and outside of the IT function.	0	1	2	3	4	5
4.13	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(PO5) Manage the Information Technology Investment						
Business Need:	Ensure funding and control of financial resource disbursement						
#	**Questions**	**Response**					
5.1	A budgeting process is in place in which an annual operating budget is established and approved that is in line with the organization's long- and short-term plans. Alternatives for funding are also investigated.	0	1	2	3	4	5
5.2	A cost monitoring process is in place that report actual figures versus budgeted figures. Possible benefits derived from the IT are also reported on.	0	1	2	3	4	5
5.3	Is a management control in place that justifies that the cost of delivering of IT services is in line with industry?	0	1	2	3	4	5
5.4	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(PO6) Communicate Management Aims and Direction						
Business Need:	To ensure user awareness and understanding of those aims						
#	**Questions**	**Response**					
6.1	A framework is in place that creates a positive control environment within the organization, creating awareness, providing guidance and removing temptation for unethical behaviour about IT related issues. Attention is also given to security and continuity issues	0	1	2	3	4	5
6.2	It is management's responsibility to develop and maintain policies regarding general aims and directives. These policies are also communicated, understood and agreed to by all levels of the organization	0	1	2	3	4	5
6.3	Proper planning is performed for allocation of resources in order to implement policies.	0	1	2	3	4	5
6.4	Policies are periodically evaluated, according to a set framework, and updated to accommodate changing conditions.	0	1	2	3	4	5
6.5	Procedures are in place to ensure that employees understand the policies and that they are being followed	0	1	2	3	4	5
6.6	A quality philosophy has been defined, documented and is maintained that is consistent with the organizational policies and philosophies.	0	1	2	3	4	5
6.7	Management has developed and is maintaining a framework policy regarding the organization's overall approach to security and internal control to protect the IT resources. This policy complies with business objectives and is aimed towards the minimizing of risks through preventative measures, timely identification and the limitation of losses. This policy is implemented at all levels within the organization.	0	1	2	3	4	5
6.8	A written policy is in place that governs the intellectual property rights on in-house and contract-developed software	0	1	2	3	4	5
6.9	Issue-specific policies are in place governing the acceptable and unacceptable use of various activities, systems and applications, as decided upon by management	0	1	2	3	4	5
6.10	An IT awareness program is in place that communicates each security policy to every IT user and to assure full understanding of the importance of IT security. This program is supported by and represent the view of management	0	1	2	3	4	5
6.11	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(PO7) Manage Human Resources
Business Need:	Acquire a competent and motivated workforce to maximize the IT process

#	**Questions**	**Response**					
7.1	The recruiting and promotion of personnel are based on objective criteria and take education, responsibility and experience into account	0	1	2	3	4	5
7.2	Personnel performing specific tasks are qualified by means of education, experience or training as required.	0	1	2	3	4	5
7.3	Roles and responsibilities have been clearly defined by management and these include the responsibility to adhere to policies, responsibility towards information security and internal control.	0	1	2	3	4	5
7.4	Employees are given orientation upon hiring and ongoing training to retain their knowledge and abilities to perform efficiently and effectively.	0	1	2	3	4	5
7.5	To prevent key IT personnel being unavailable, cross-training and backup are provided by management. Personnel in sensitive positions are required to take uninterrupted holidays of sufficient length to exercise the organization's ability to cope with the unavailability and to prevent and detect fraudulent activity.	0	1	2	3	4	5
7.6	Personnel being hired or promoted undergo a security clearance procedure, depending on the sensitivity of their position.	0	1	2	3	4	5
7.7	Employees' performance is regularly evaluated on a performance and reward bases connecting their performance to the organization's overall performance.	0	1	2	3	4	5
7.8	Appropriate and timely actions are taken to ensure that job changes and terminations do not impair internal controls regarding Information Security within the organization.	0	1	2	3	4	5
7.9	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(PO8) Compliance with external requirements						
Business Need:	To meet legal, regulatory and contractual obligations						
#	Questions	Response					
8.1	Procedures are established to review external requirements. Management review the impact of any external relationship on the organization's information needs in order to determine is IT strategies should be adjusted to conform to these relationships.	0	1	2	3	4	5
8.2	Corrective actions are regularly, or on a timely basis, performed to ensure that the organization comply with external requirements. Legal advice is also obtained if required.	0	1	2	3	4	5
8.3	Safety and ergonomic standards are complied with in the working environment of IT users and staff.	0	1	2	3	4	5
8.4	Issues such as privacy, intellectual property and cryptographic practices are complied with by the organization and is endorsed by management	0	1	2	3	4	5
8.5	Formal contracts for electronic commerce are in place that establishes agreement between the organization and its trading partners regarding communication practices and transaction message security and data storage. If trading on the Internet, controls are in place ensuring compliance with local and world-wide regulations.	0	1	2	3	4	5
8.6	Insurance contract requirements are identified and continuously met.	0	1	2	3	4	5
8.7	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(PO9) Assess Risks						
Business Need:	To achieve business objectives and respond to threats.						
#	**Questions**	**Response**					
9.1	A business risk assessment framework has been established and incorporates from regular assessments of information risks to the achievement of business objectives.	0	1	2	3	4	5
9.2	A general risk assessment approach is followed where scope, boundaries and a methodology is defined for performing the assessment. Management leads the identification of suitable risk mitigation solutions whereas security specialists lead the identification of threats to information assets.	0	1	2	3	4	5
9.3	The risk assessment approach focuses on the essential elements of risk and the cause-and-effect relationship between them. These elements include: tangible and intangible assets, asset value, threats, vulnerabilities, safeguards, consequences and the likelihood of a threat. They are ranked by quantitative and qualitative measures. Management input is considered important.	0	1	2	3	4	5
9.4	The risk acceptance capacity of the organization, as well as quantitative measures to which an area is exposed, is the result of risk assessment.	0	1	2	3	4	5
9.5	A risk action plan is in place ensuring that cost-effective controls and security measures mitigate risk continuously. This plan also states the risk strategy towards risk in terms of acceptance, mitigation or avoidance.	0	1	2	3	4	5
9.6	The risk assessment approach ensures that residual risk is formally accepted (depending on risk identification, measurement, organizational policies, uncertainty and the cost-effectiveness of implementing safeguards and controls) and is offset with adequate insurance coverage, contracted liabilities or self-insurance.	0	1	2	3	4	5
9.7	The control system balances prevention, detection, correction and recovery measures. Management communicates the purpose of these controls, manage conflicting control measures and monitor the effectiveness of applied safeguard controls.	0	1	2	3	4	5
9.8	Risk assessment is highly encouraged in the organization as an important tool providing information about the design and implementation about internal controls, the definition of the	0	1	2	3	4	5

	strategic IT plan as well as the monitoring and evaluation mechanisms.						
9.9	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(PO10) Manage Projects						
Business Need:	To set priorities, deliver on time and within budget						
#	**Questions**	**Response**					
10.1	A general project management framework defines the scope and boundaries of managing projects as well as the methodology to be applied to every project. This methodology include: Responsibilities, task breakdown, budgeting, milestones and checkpoints of approval.	0	1	2	3	4	5
10.2	The project management framework provides for input and participation by the affected user department's management in the definition and authorization of a development, implementation or modification project.	0	1	2	3	4	5
10.3	The responsibilities and authorities of project team members, as well as the basis for assigning staff to a project are defined in the project management framework.	0	1	2	3	4	5
10.4	Before work on any project begins, a clear and written statement is created that states the nature and scope of the project	0	1	2	3	4	5
10.5	Every proposed project is reviewed by senior management for feasibility and whether to commence with the project.	0	1	2	3	4	5
10.6	Completed work is approved by designated managers in each phase before work on the next phase begins.	0	1	2	3	4	5
10.7	A project master plan is created for each approved project. This plan include all the elements of the project planning process, including: Scope statements, time and resource allocation, responsibilities etc.	0	1	2	3	4	5
10.8	The implementation of a new or modified system includes a quality plan, integrated with the master project plan and is formally reviewed and accepted by all concerned parties.	0	1	2	3	4	5
10.9	Assurance tasks are identified in the planning phase and it supports the accreditation of new or modified systems and that internal controls and security features meet the related requirements	0	1	2	3	4	5
10.10	A formal project risk management program is in place for each individual project that eliminates or minimizes project-related risks.	0	1	2	3	4	5

10.11	A test plan is created for every development, implementation or modification project.	0	1	2	3	4	5
10.12	A training plan is created for every development, implementation or modification project.	0	1	2	3	4	5
10.13	A post-implementation plan is created for every new or modification project to determine whether the project has delivered the planned benefits.	0	1	2	3	4	5
10.14	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(PO11) Manage quality						
Business Need:	To meet IT customer requirements						
#	**Questions**	**Response**					
11.1	Management develops and regularly maintains an overall quality plan that is based on the organization's long- and short-term plans.	0	1	2	3	4	5
11.2	A standard approach exists regarding quality assurance for both general and project-specific quality assurance activities. It prescribes reviews, audits and inspections to be performed in order to achieve the requirements of the quality plan.	0	1	2	3	4	5
11.3	The scope and timing of quality assurance activities are planned as part of a quality assurance planning process.	0	1	2	3	4	5
11.4	Quality assurance personnel's responsibilities include a general review of general adherence to IT standards and procedures.	0	1	2	3	4	5
11.5	Management has defined and implemented standards and has adopted a development methodology that governs each phase of the project, as well as appropriate for each type of project	0	1	2	3	4	5
11.6	In the event of major changes are made to existing technology, the development life cycle are observed, as in the case of development or acquisition of new technology	0	1	2	3	4	5
11.7	The systems development methodology is periodically reviewed to ensure that it reflects current generally accepted techniques and procedures.	0	1	2	3	4	5
11.8	A process is established ensuring close communication and coordination between the customers of IT and the system implementers. Management also promotes an organization where close coordination and communication are intricate to the	0	1	2	3	4	5

	systems development life cycle						
11.9	An acquisition and maintenance framework exists governing the acquiring, programming, documenting, testing, parameter setting, maintenance and applying fixes to the IT infrastructure.	0	1	2	3	4	5
11.10	Management implements a process that ensures good relationships with third-party implementers. It provides that the user and implementer agree to criteria such as acceptance, handling of changes, development problems, user roles, facilities, tools etc.	0	1	2	3	4	5
11.11	Documentation that is developed in development and modification projects conform to a predefined standard, as communicated by from management.	0	1	2	3	4	5
11.12	The systems development life cycle methodology provides standards on testing requirements, verification and documentation for **unit testing** as part of every development or modification project	0	1	2	3	4	5
11.13	The systems development life cycle methodology provides standards on testing requirements, verification, and documentation for the **total system testing** as part of every development or modification project.	0	1	2	3	4	5
11.14	The methodology defines circumstances under which pilot or parallel testing of new and/or existing systems will be performed.	0	1	2	3	4	5
11.15	After every development or modification project, the documented results of testing the system are retained.	0	1	2	3	4	5
11.16	The quality assurance approach requires that a post-implementation review be conducted of an operational system to determine whether the project team adhered to the provisions of the development methodology	0	1	2	3	4	5
11.17	The quality assurance approach includes a review of which particular systems and development activities have achieved the objectives of the Information Services function.	0	1	2	3	4	5

11.18	Management-defined metrics are used to measure the results of activities, thus assessing whether quality goals have been achieved	0	1	2	3	4	5
11.19	Reports of quality assurance review meetings are prepared and submitted to management of user departments and of the IT function	0	1	2	3	4	5
11.20	How relevant is this IT process to your organization?	0	1	2	3	4	5

CobiT Domain: Acquire and Implementation (AI)

Business Process:	(AI1) Identify automated solutions
Business Need:	Ensure an effective and efficient approach to satisfy user requirements

#	Questions	Response					
12.1	The systems development methodology provides that the requirements that are satisfied by the current systems, as well as those requirements that have to be satisfied by new or modified systems are clearly defined before the project is approved.	0	1	2	3	4	5
12.2	Alternate courses of action are also analyzed and evaluated for a proposed new or modified system.	0	1	2	3	4	5
12.3	The acquisition strategy for new or modified systems is in line with the organization's long- and short-term plans. For software acquisition, a strategy plan indicates whether software will be developed in-house, bought off-the-shelf or through a contract.	0	1	2	3	4	5
12.4	The development methodology provides for the evaluation of requirements and specifications for a request-for-proposal when dealing with third-party service vendors.	0	1	2	3	4	5
12.5	For each proposed alternative for proposed new or modification projects, a technological feasibility study (keeping in mind the organization's data model) as well as an economic feasibility study is conducted for satisfying user requirements, as well as the cost and benefits involved.	0	1	2	3	4	5
12.6	For every proposed new or development project, security threats, potential vulnerabilities, impacts, feasible security and internal controls are defined and analyzed. This is done in line with the overall Risk Management framework.	0	1	2	3	4	5
12.7	Management ensures that the costs and benefits of security are carefully examined to ensure that the cost of security controls does not exceed the benefits. This decision is formally signed off by Management.	0	1	2	3	4	5
12.8	Mechanisms for adequate audit trails are available or can be developed. These mechanisms provide the abilities to protect sensitive data against misuse	0	1	2	3	4	5
12.9	For development, implementation or modification IT projects, the IT function takes into account ergonomic issues that is associated with the introduction of automated systems.	0	1	2	3	4	5

12.10	A standard procedure is followed and adhered to by the IT function to identify all system software programs that will satisfy all its operational requirements	0	1	2	3	4	5
12.11	Management has developed a central procurement approach describing a common set of procedures and standards to be followed in the procurement of information technology related hardware, software and services. Products are reviewed and tested prior to their use and payment.	0	1	2	3	4	5
12.12	Software product acquisition follows the organization's procurement policies.	0	1	2	3	4	5
12.13	Management requires that for licensed software acquired from third-party providers, the providers have appropriate procedures to validate, protect and maintain the software product's integrity rights. Consideration is given to the support of the product in any maintenance agreement related to the delivered product.	0	1	2	3	4	5
12.14	The procurement of contract programming services is justified with a written request for services from a designated member of the IT function. The contract stipulates that the software, documentation and other deliverables are subject to testing and review prior to acceptance. The product is also tested against standards by the IT function's quality assurance group.	0	1	2	3	4	5
12.15	An acceptance plan for facilities, as well as for technology to be provided is agreed upon with the supplier in the contract and this plan defines the acceptance procedures and criteria. In addition, acceptance tests are performed to guarantee that the accommodation and environment meet the requirements, as well as functionality and workload tests, as specified in the contract.	0	1	2	3	4	5
12.16	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(AI2) Acquire and Maintain application software
Business Need:	Providing automated functions which effectively support the business process.

#	Questions	Response					
13.1	Appropriate procedures and techniques, involving close collaboration with system users, are applied to create the design specifications for each new information system development project and to verify the design specifications against the user requirements.	0	1	2	3	4	5
13.2	In the event of major changes to existing systems, a similar development process is observed as in the case of the development of new systems.	0	1	2	3	4	5
13.3	The organization's system development life cycle methodology requires that the design specifications for all information system development and modification projects are reviewed and approved by management, the affected user departments and the organization's senior management, when appropriate.	0	1	2	3	4	5
13.4	An appropriate procedure is applied for defining and documenting the file format for each information system development or modification project. This procedure ensures that the data dictionary rules are respected.	0	1	2	3	4	5
13.5	Detailed written program specifications are prepared for each information system development or modification project.	0	1	2	3	4	5
13.6	Adequate mechanisms for the collection and entry of data are specified for each information system development or modification project.	0	1	2	3	4	5
13.7	Adequate mechanisms exist for defining and documenting the input requirements for each information system development or modification project.	0	1	2	3	4	5
13.8	All external and internal interfaces are properly specified, designed and documented.	0	1	2	3	4	5

13.9	The organization's system development life cycle methodology provides for the development of an easy to use, self-documenting interface between the user and machine (by means of online help functions).	0	1	2	3	4	5
13.10	Adequate mechanisms exist for defining and documenting the processing, as well as output requirements for each information system development or modification project.	0	1	2	3	4	5
13.11	Adequate mechanisms for assuring the internal control and security requirements are specified for each information system development or modification project. Information systems are designed to include application controls which guarantee the accuracy, completeness, timeliness and authorization of inputs, processing and outputs.	0	1	2	3	4	5
13.12	Availability is considered in the design process for new or modified information systems at the earliest possible stage. Availability is analyzed and, if necessary, increased through maintainability and reliability improvements.	0	1	2	3	4	5
13.13	Established procedures exist to assure, where applicable, that application programs routinely verify the tasks performed by the software to help assure data integrity, and which provide the restoration of the integrity through rollback, recovery or other means.	0	1	2	3	4	5
13.14	Unit testing, application testing, integration testing, system testing, and load and stress testing are performed according to the project test plan and established testing standards before it is approved by the user. Adequate measures are conducted to prevent disclosure of sensitive information used during testing.	0	1	2	3	4	5
13.15	Adequate user reference and support manuals are prepared (preferably in electronic format) as part of every information system development or modification project.	0	1	2	3	4	5
13.16	The system design is reassessed whenever significant technical and/or logical discrepancies occur during system development or maintenance.	0	1	2	3	4	5

13.17	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(AI3) Acquire and Maintain Technology Infrastructure						
Business Need:	Providing the appropriate platforms to support business applications.						
#	**Questions**	**Response**					
14.1	Hardware and software selection criteria are based on the functional specifications for the new or modified system and identify mandatory and optional requirements. The impact of the new additions to the system is assessed in terms of overall system performance.	0	1	2	3	4	5
14.2	IT management schedules routine and periodic hardware maintenance to reduce the frequency and impact of performance failures.	0	1	2	3	4	5
14.3	IT management ensures that the set-up of system software to be installed does not jeopardize the security of the data and programs being stored on the system.	0	1	2	3	4	5
14.4	System software is installed in accordance with the acquisition and maintenance framework for the technology infrastructure. Testing is performed before use of the software in the production environment is authorized.	0	1	2	3	4	5
14.5	System software is maintained in accordance with the acquisition and maintenance framework for the technology infrastructure.	0	1	2	3	4	5
14.6	System software changes are controlled in line with the organization's change management procedures.	0	1	2	3	4	5
14.7	Policies and techniques are implemented for using, monitoring and evaluating the use of system utilities. Responsibilities for using sensitive software utilities are clearly defined and understood by developers, and the use of the utilities are monitored and logged.	0	1	2	3	4	5
14.8	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(AI4) Develop and Maintain Procedures						
Business Need:	Ensuring the proper use of the applications and the technological solutions put in place.						
#	**Questions**	**Response**					
15.1	The organization's system development life cycle methodology ensures the timely definition of operational requirements and service levels.	0	1	2	3	4	5
15.2	Adequate user procedures manuals are prepared and refreshed as part of every information system development, implementation or modification project.	0	1	2	3	4	5
15.3	An adequate operations manual is prepared and kept up-to-date as part of every information system development, implementation or modification project.	0	1	2	3	4	5
15.4	Adequate training materials are developed as part of every information system development, implementation or modification project. These materials focus on the system's use in daily practice.	0	1	2	3	4	5
15.5	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(AI5) Install and Accredit systems						
Business Need:	Verify and confirm that the solution is fit for the intended purpose.						
#	**Questions**	**Response**					
16.1	Staff of the affected user departments, as well as the operations group of the IT function is trained in accordance with the defined training plan and associated materials, as part of every information systems development, implementation or modification project.	0	1	2	3	4	5
16.2	Application software performance optimization is established as an integral part of the organization's system development life cycle methodology to forecast the resources required for operating new and significantly changed software.	0	1	2	3	4	5

16.3	An implementation plan is prepared, reviewed and approved by relevant parties and be used to measure progress. The implementation plan addresses site preparation, equipment acquisition and installation, user training, installation of operating software changes, implementation of operating procedures and conversion.	0	1	2	3	4	5
16.4	As part of every information system development, implementation or modification project, the necessary elements from the old system are converted to the new one according to a pre-established plan.	0	1	2	3	4	5
16.5	A data conversion plan is prepared, defining the methods of collecting and verifying the data to be converted and identifying and resolving any errors found during conversion.	0	1	2	3	4	5
16.6	Testing strategies and plans are prepared and signed off by the system owner and IT management.	0	1	2	3	4	5
16.7	Changes are tested in accordance with the impact and resource assessment in a separate test environment by an independent (from builders) test group before use in the regular operational environment begins. Back-out plans are also developed. Acceptance testing is carried out in an environment that is representative of the future operational environment.	0	1	2	3	4	5
16.8	Parallel or pilot testing is performed in accordance with a pre-established plan and the criteria for terminating the testing process are specified in advance.	0	1	2	3	4	5
16.9	As part of the final acceptance or quality assurance testing of new or modified information systems, a formal evaluation and approval of the test results is required by management of the affected user department(s) and the IT function. The tests cover all components of the information system (e.g., application software, facilities, technology, user procedures).	0	1	2	3	4	5
16.10	Management has defined and implements procedures to ensure that operations and user management formally accept the test results and the level of security for the systems, along with the remaining residual risk.	0	1	2	3	4	5

16.11	Before moving the system into operation, the user or designated custodian validates its operation as a complete product, under conditions and in the manner similar to the production environment.	0	1	2	3	4	5
16.12	Management has defined and implements formal procedures to control the handover of the system from development to testing to operations.	0	1	2	3	4	5
16.13	A post-implementation review of operational information system requirements (e.g., capacity, throughput, etc.) is conducted to assess whether the users' needs are being met by the system.	0	1	2	3	4	5
16.14	A post-implementation review of an operational information system is conducted to assess and report on whether the system delivered the benefits envisioned in the most cost-effective manner.	0	1	2	3	4	5
16.15	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(AI6) Manage changes						
Business Need:	Minimizing the likelihood of disruption, unauthorized alterations and errors.						
#	**Questions**	**Response**					
17.1	All requests for changes, system maintenance and supplier maintenance are standardized and are subject to formal change management procedures. Consideration is given to urgent matters, as well as status reports.	0	1	2	3	4	5
17.2	All requests for change are assessed in a structured way for all possible impacts on the operational system and its functionality.	0	1	2	3	4	5
17.3	Change management and software control and distribution are properly integrated with a comprehensive configuration management system.	0	1	2	3	4	5
17.4	IT management has established parameters defining emergency changes and procedures to control these changes when they circumvent the normal process of technical, operational and management assessment prior to implementation.	0	1	2	3	4	5

	The emergency changes are recorded and authorized by IT management prior to implementation.						
17.5	The change process ensures that whenever system changes are implemented, the associated documentation and procedures are updated accordingly.	0	1	2	3	4	5
17.6	Maintenance personnel have specific assignments and their work is properly monitored. Their system access rights are controlled to avoid risks of unauthorized access to automated systems.	0	1	2	3	4	5
17.7	The release of software is governed by formal procedures ensuring sign-off, packaging, regression testing, handover, etc.	0	1	2	3	4	5
17.8	Specific internal control measures are established to ensure distribution of the correct software element to the right place, with integrity, and in a timely manner with adequate audit trails.	0	1	2	3	4	5
17.9	How relevant is this IT process to your organization?	0	1	2	3	4	5

CobiT Domain: Delivery and Support (DS)

Business Process:	(DS1) Define and Manage Service Levels						
Business Need:	Establish a common understanding of the level of service required						
#	**Questions**	**Response**					
18.1	Management has defined formal service level agreements and defines the minimal contents such as: availability, reliability, performance, growth capacity, level of support provided, security, continuity planning, restrictions etc. Users and the IT function have a written agreement which describes the service level in qualitative and quantitative terms. The agreement defines the responsibilities of both parties.	0	1	2	3	4	5
18.2	Agreement has been reached about which aspects a service level agreement should contain. At minimum, a service level agreement contain: availability, reliability, performance, growth capacity, level of support provided, security, continuity planning, restrictions etc.	0	1	2	3	4	5
18.3	Procedures are in place to ensure that the manner of and responsibilities for performance governing relations (e.g., non-disclosure agreements) between all the involved parties are established, coordinated, maintained and communicated to all affected departments.	0	1	2	3	4	5
18.4	A service level manager has been appointed who is responsible for monitoring and reporting on the achievement of the specified service performance criteria and all problems encountered during processing. The monitoring statistics are analyzed on a timely basis. Appropriate corrective action is taken and failures investigated.	0	1	2	3	4	5
18.5	Management regularly reviews service level agreements and underpinning contracts with third-party service providers.	0	1	2	3	4	5
18.6	Provisions for chargeable items are included in the service level agreements to make trade-offs possible between service levels and costs.	0	1	2	3	4	5
18.7	Management ensures that users and service level managers regularly agree on a service improvement program for pursuing	0	1	2	3	4	5

	cost-justified improvements to the service level.						
18.8	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(DS2) Manage Third-party services						
Business Need:	Roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements.						
#	**Questions**	**Response**					
19.1	All third-party providers' services are properly identified and the technical and organizational interfaces with suppliers are documented.	0	1	2	3	4	5
19.2	The customer organization management has an appointed relationship owner who is responsible for ensuring the quality of the relationships with third-parties.	0	1	2	3	4	5
19.3	For each relationship with a third party service provider, a formal contract is defined and agreed upon before work starts.	0	1	2	3	4	5
19.4	Before selection, potential third-parties are properly qualified through an assessment of their capability to deliver the required service (due diligence).	0	1	2	3	4	5
19.5	The contract between the facilities management provider and the organization is based on required processing levels, security, monitoring and contingency requirements, and other stipulations as appropriate.	0	1	2	3	4	5
19.6	With respect to ensuring continuity of services, management considers business risk related to the third-party in terms of legal uncertainties and the going concern concept, and negotiates escrow contracts where appropriate.	0	1	2	3	4	5
19.7	Security agreements (e.g. non-disclosure agreements) are identified and explicitly stated and agreed to, and conform to universal business standards in accordance with legal and regulatory requirements, including liabilities.	0	1	2	3	4	5
19.8	Service delivery of the third-party is monitored to ensure the continuing adherence to the contract agreements.	0	1	2	3	4	5

19.9	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(DS3) Manage performance and capacity
Business Need:	Adequate capacity is available and that best and optimal use is made of it to meet required performance needs.

#	**Questions**	**Response**					
20.1	Business needs are identified regarding availability and performance of information services and converted into availability terms and requirements.	0	1	2	3	4	5
20.2	An availability plan is established to achieve, monitor and control the availability of information services.	0	1	2	3	4	5
20.3	The performance of IT resources is continuously monitored and exceptions are reported in a timely and comprehensive manner.	0	1	2	3	4	5
20.4	Appropriate modeling tools were used to produce a model of the current system which has been calibrated and adjusted against actual workload and is accurate within recommended load levels. Modeling tools are used to assist with the prediction of capacity, configuration reliability, performance and availability requirements.	0	1	2	3	4	5
20.5	The performance management process includes forecasting capability to enable problems to be corrected before they affect system performance.	0	1	2	3	4	5
20.6	Controls are in place to ensure that workload forecasts are prepared to identify trends and to provide information needed for the capacity plan.	0	1	2	3	4	5
20.7	Hardware performance and capacity are reviewed to ensure that cost-justifiable capacity always exists to process the agreed workloads and to provide the required performance quality and quantity prescribed in service level agreements. The capacity plan covers multiple scenarios.	0	1	2	3	4	5
20.8	Fault tolerance mechanisms, prioritizing tasks and equitable resource allocation mechanisms are implemented to prevent resources from being unavailable, after availability requirements	0	1	2	3	4	5

	have been identified.						
20.9	Management ensures for the timely acquisition of required capacity, taking into account aspects such as resilience, contingency, workloads and storage plans.	0	1	2	3	4	5
20.10	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(DS4) Ensure continuous service						
Business Need:	IT services are available as required and to ensure a minimum business impact in the event of a major disruption						
#	**Questions**	**Response**					
21.1	IT management and business process owners has established a continuity framework which defines the roles, responsibilities and the risk-based approach/methodology to be adopted, and the rules and structures to document the continuity plan as well as the approval procedures.	0	1	2	3	4	5
21.2	The IT continuity plan is in line with the overall business continuity plan to ensure consistency. Furthermore, the IT continuity plan takes into account the IT long- and short-range plans to ensure consistency.	0	1	2	3	4	5
21.3	IT management has developed a written plan containing the following: • Guidelines on how to use the continuity plan • Emergency procedures to ensure the safety of all affected staff members • Response procedures meant to bring the business back to the state it was in before the incident or disaster • Recovery procedures meant to bring the business back to the state it was in before the incident or disaster • Procedures to safeguard and reconstruct the home site • Co-ordination procedures with public authorities • Communication procedures with stakeholders, employees, key customers, critical suppliers, stockholders and management • Critical information on continuity teams, affected staff, customers, suppliers, public, authorities and media	0	1	2	3	4	5

21.4	Procedures and guidelines are established for minimizing the continuity requirements with regard to personnel, facilities, hardware, software, equipment, forms, supplies and furniture.	0	1	2	3	4	5
21.5	Change control procedures in order to ensure that the continuity plan is up-to-date and reflects actual business requirements. This requires continuity plan maintenance procedures aligned with change and management and human resources procedures.	0	1	2	3	4	5
21.6	To have an effective continuity plan, management assesses its adequacy on a regular basis or upon major changes to the business or IT infrastructure; this is done with careful preparation, documentation, reporting test results and, according to the results, implementing an action plan.	0	1	2	3	4	5
21.7	All concerned parties receive regular training sessions regarding the procedures to be followed in case of an incident or disaster.	0	1	2	3	4	5
21.8	Since the information in the disaster recovery plan is sensitive, it is distributed only to authorized personnel and is safeguarded against unauthorized disclosure. Sections of the plan are distributed on a need-to-know basis.	0	1	2	3	4	5
21.9	User departments have established alternative processing procedures that may be used until the IT function is able to fully restore its services after a disaster or an event.	0	1	2	3	4	5
21.10	The continuity plan identifies the critical application programs, third-party services, operating systems, personnel and supplies, data files and time frames needed for recovery after a disaster occurs. Critical data and operations have been identified, documented, prioritized and approved by the business process owners, in cooperation with IT management.	0	1	2	3	4	5
21.11	The continuity plan identifies alternatives regarding the back-up site and hardware as well as a final alternative selection. If applicable, a formal contract for these types of services should be concluded.	0	1	2	3	4	5
21.12	Off-site storage of critical back-up media, documentation and other IT resources are established to support recovery and business continuity plans. Business process owners and IT	0	1	2	3	4	5

	function personnel are involved in determining what back-up resources need to be stored off-site. Environmental and security protection are also determined and assessed on a regular basis.						
21.13	On successful resumption of the IT function after a disaster, IT management assesses the adequacy of the plan and updates it accordingly.	0	1	2	3	4	5
21.14	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(DS5) Ensure Systems Security						
Business Need:	Safeguard information against unauthorized use, disclosure or modification, damage or loss						
#	**Questions**	**Response**					
22.1	IT security is managed so that security measures are in line with business requirements. This includes: • Translating risk assessment information to the IT security plans • Implementing the IT security plan • Updating the IT security plan to reflect changes in the IT configuration • Assessing the impact of change requests on IT security • Monitoring the implementation of the IT security plan • Aligning IT security procedures to other policies and procedures	0	1	2	3	4	5
22.2	The logical access to and use of IT computing resources are restricted by the implementation of adequate identification, authentication and authorization mechanisms, linking users and resources with access rules. Procedures are in place to keep authentication and access mechanisms effective (e.g., regular password changes).	0	1	2	3	4	5
22.3	IT management implements procedures in line with the security policy that provides access security control based on the individual's demonstrated need to view, add, change or delete data.	0	1	2	3	4	5
22.4	Management has established procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts. A formal approval procedure outlining	0	1	2	3	4	5

	the data or system owner granting the access privileges are included.						
22.5	A control process is in place to review and confirm access rights periodically. Periodic comparison of resources with recorded accountability is made to help reduce the risk of errors, fraud, misuse or unauthorized alteration.	0	1	2	3	4	5
22.6	Users systematically control the activity of their proper account(s). Also information (monitoring and reporting) mechanisms are in place to allow them to oversee normal activity as well as to be alerted to unusual activity in a timely manner.	0	1	2	3	4	5
22.7	Security activity is logged and any indication of imminent security violation is reported immediately to all who may be concerned, internally and externally, and is acted upon in a timely manner.	0	1	2	3	4	5
22.8	All data are classified in terms of sensitivity by a formal and explicit decision by the data owner according to the data classification scheme. Even data needing “no protection” requires a formal decision to be so designated. Evidence of owner approval and data disposition are maintained.	0	1	2	3	4	5
22.9	Controls are in place to ensure that the identification and access rights of users as well as the identity of system and data ownership are established and managed in a unique and central manner to obtain consistency and efficiency of global access control.	0	1	2	3	4	5
22.10	Violation and security activity is logged, reported, reviewed and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorized activity. The logical access to the computer resources accountability information (security and other logs) is granted based upon the principle of least privilege, or need-to-know.	0	1	2	3	4	5
22.11	Incident management responsibilities and procedures are established to ensure an appropriate, effective and timely response to security incidents.	0	1	2	3	4	5

22.12	Reaccreditation of security (e.g., through "tiger teams") is periodically performed to keep the formally approved security level and the acceptance of residual risk up-to-date.	0	1	2	3	4	5
22.13	Control practices are implemented to verify the authenticity of the counterparty providing electronic instructions or transactions. This can be implemented through trusted exchange of passwords, tokens or cryptographic keys.	0	1	2	3	4	5
22.14	Where appropriate, controls are implemented to provide authenticity of transactions and establish the validity of a user's claimed identity to the system. This is performed with cryptographic techniques for signing and verifying transactions.	0	1	2	3	4	5
22.15	Organizational policy ensures that, where appropriate, transactions cannot be denied by either party, and controls are implemented to provide non-repudiation of origin or receipt, proof of submission, and receipt of transactions.	0	1	2	3	4	5
22.16	Sensitive transaction data is only exchanged over a trusted path. Sensitive information includes security management information, sensitive transaction data, passwords and cryptographic keys.	0	1	2	3	4	5
22.17	All security related hardware and software are at all times protected against tampering to maintain their integrity and against disclosure of secret keys. In addition, the organization keeps a low profile about their security design,	0	1	2	3	4	5
22.18	Procedures and protocols are implemented to be used for generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorized disclosure.	0	1	2	3	4	5
22.19	Adequate preventative, detective, corrective control, occurrence response and reporting measures regarding malicious software, such as computer viruses or trojan horses, are in place to protect information systems and technology from these software threats.	0	1	2	3	4	5
22.20	Regarding the Internet or other public network connection, adequate firewalls are operative to protect against denial of	0	1	2	3	4	5

	services and any unauthorized access to the internal resources;						
22.21	Management protects the continued integrity of all cards or similar physical mechanisms used for authentication or storage of financial or other sensitive information, taking into consideration the related facilities, devices, employees and validation methods used.	0	1	2	3	4	5
22.22	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(DS6) Identify and Allocate costs
Business Need:	Ensuring a correct awareness of the costs attributable to IT services

#	**Questions**	**Response**					
23.1	Chargeable items are identifiable, measurable and predictable by users. Users are able to control the use of information services and associated billing levels.	0	1	2	3	4	5
23.2	IT management implements costing procedures to provide management information on the costs of delivering information services while ensuring cost effectiveness. Variances between forecasts and actual costs are reported on to facilitate the cost monitoring.	0	1	2	3	4	5
23.3	IT management has defined and uses billing and chargeback procedures. It maintains user billing and chargeback procedures that encourage the proper usage of computer resources and assure the fair treatment of user departments and their needs.	0	1	2	3	4	5
23.4	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(DS7) Educate and train users
Business Need:	Ensuring that users are making effective use of technology and are aware of the risks and responsibilities involved.

#	**Questions**	**Response**					
24.1	In line with the long-range plan, management has established procedures for identifying and documenting the training needs of	0	1	2	3	4	5

	all personnel using information services. A training curriculum for each group of employees is established.						
24.2	Based on the identified needs, management has defined the target groups, identified and appointed trainers, and organizes timely training sessions.	0	1	2	3	4	5
24.3	All personnel are trained and educated in system security principles, including periodic updates with special focus on security awareness and incident handling.	0	1	2	3	4	5
24.4	Management provides an education and training program that includes: ethical conduct of the IT function, security practices to protect against harm from failures affecting availability, confidentiality, integrity and performance of duties in a secure manner.	0	1	2	3	4	5
24.5	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(DS8) Assist and Advise customers						
Business Need:	Ensuring that any problem experienced by the user is appropriately resolved.						
#	**Questions**	**Response**					
25.1	User support is established within a "help desk" function. Individuals responsible for performing this function closely interact with problem management personnel.	0	1	2	3	4	5
25.2	All customer queries are adequately registered by the help desk.	0	1	2	3	4	5
25.3	Customer queries which cannot immediately be resolved are appropriately escalated within the IT function.	0	1	2	3	4	5
25.4	The clearance of customer queries is monitored in a timely manner. Long outstanding queries are investigated and acted upon.	0	1	2	3	4	5
25.5	Adequate reporting is done with regard to customer queries and resolution, response times and trend identification. The reports are adequately analyzed and acted upon.	0	1	2	3	4	5
25.6	How relevant is this IT function to your organization?	0	1	2	3	4	5

Business Process:	(DS9) Manage the configuration						
Business Need:	Accounting for all IT components, prevent unauthorized alterations, verify physical existence and provide a basis for sound change management.						
#	**Questions**	**Response**					
26.1	Procedures are in place to ensure that only authorized and identifiable configuration items are recorded in inventory upon acquisition. These procedures also provide for the authorized disposal and consequential sale of configuration items. Changes to the configuration are also kept track of.	0	1	2	3	4	5
26.2	A baseline of configuration items is kept as a checkpoint to return to after changes.	0	1	2	3	4	5
26.3	The configuration records reflect the actual status of all configuration items including the history of changes.	0	1	2	3	4	5
26.4	The existence and consistency of recording of the IT configuration is periodically checked.	0	1	2	3	4	5
26.5	Clear policies restricting the use of personal and unlicensed software have been developed and are enforced.	0	1	2	3	4	5
26.6	A file storage area (library) is defined for all valid software items in appropriate phases of the system development life cycle. These areas are separated from each other and from development, testing and production file storage areas.	0	1	2	3	4	5
26.7	Critical components of the organization's IT resources have been appropriately identified and are maintained.	0	1	2	3	4	5
26.8	Software is labeled, inventoried and properly licensed. Library management software is used to produce audit trails of program changes and to maintain program version numbers, creation-date information and copies of previous versions.	0	1	2	3	4	5
26.9	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(DS10) Manage problems and incidents
Business Need:	Problems and incidents are resolved, and the cause investigated to prevent any recurrence.

#	**Questions**	**Response**					
27.1	All operational events which are not part of the standard operation (incidents, problems and errors) are recorded, analyzed and resolved in a timely manner. Emergency program change procedures are promptly tested, documented, approved and reported. Incident reports are created in the case of significant problems.	0	1	2	3	4	5
27.2	Identified problems are solved in the most efficient way on a timely basis. These procedures ensure that problem priorities are appropriately set. The procedures also document the escalation process for the activation of the IT continuity plan.	0	1	2	3	4	5
27.3	The problem management system provides adequate audit trail facilities which allow tracing from incident to underlying cause (e.g., package release or urgent change implementation) and back. It closely interworks with change management, availability management and configuration management.	0	1	2	3	4	5
27.4	Emergency and temporary access authorizations are documented on standard forms and maintained on file, approved by appropriate managers, securely communicated to the security function and automatically terminated after a predetermined period.	0	1	2	3	4	5
27.5	Emergency processing priorities are established, documented and approved by appropriate program and IT management.	0	1	2	3	4	5
27.6	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(DS11) Manage data
Business Need:	Ensure that data remains complete, accurate and valid during its input, update and storage

#	**Questions**	**Response**					
28.1	User departments follow data preparation procedures that include appropriate input form design and error handling to minimize and report errors and enforce consistency,	0	1	2	3	4	5
28.2	Source documents are properly prepared by authorized personnel who are acting within their authority and adequate segregation of duties are in place regarding the origination and approval of source documents.	0	1	2	3	4	5
28.3	All authorized source documents are complete and accurate, properly accounted for and transmitted in a timely manner for entry.	0	1	2	3	4	5
28.4	Error handling procedures during data origination reasonably ensure that errors and irregularities are detected, reported and corrected.	0	1	2	3	4	5
28.5	Original source documents are retained or are reproducible by the organization for an adequate amount of time to facilitate retrieval or reconstruction of data as well as to satisfy legal requirements.	0	1	2	3	4	5
28.6	Data input is performed only by authorized staff.	0	1	2	3	4	5
28.7	Transaction data entered for processing (people-generated, system-generated or interfaced inputs) are subject to a variety of controls to check for accuracy, completeness and validity as close to the point of origination as possible.	0	1	2	3	4	5
28.8	Procedures are established for the correction and resubmission of data which was erroneously input.	0	1	2	3	4	5
28.9	Separation of duties is maintained and that work performed is routinely verified. Adequate update controls such as run-to-run control totals and master file update controls are in place.	0	1	2	3	4	5

28.10	Data processing validation, authentication and editing are performed as close to the point of origination as possible.	0	1	2	3	4	5
28.11	Erroneous transactions are identified without being processed and without undue disruption of the processing of other valid transactions.	0	1	2	3	4	5
28.12	Established procedures exist for the handling and retention of output from its IT application programs. In case of negotiable instruments (e.g., value cards) are the output recipients, special care are taken to prevent misuse.	0	1	2	3	4	5
28.13	The organization established and communicates written procedures for the distribution of IT output.	0	1	2	3	4	5
28.14	Output is routinely balanced to the relevant control totals. Audit trails facilitate the tracing of transaction processing and the reconciliation of disrupted data.	0	1	2	3	4	5
28.15	The accuracy of output reports is reviewed by the provider and the relevant users. Errors contained in the output are monitored, reported and rectified.	0	1	2	3	4	5
28.16	The security of output reports is maintained for those awaiting distribution, as well as those already distributed to users.	0	1	2	3	4	5
28.17	Adequate protection of sensitive information is provided during transmission and transport against unauthorized access, modification and misaddressing.	0	1	2	3	4	5
28.18	Access to sensitive information and software from computers, disks and other equipment or media is prevented when they are disposed of or transferred to another use. These procedures guarantee that data marked as deleted or to be disposed cannot be retrieved by any internal or third party.	0	1	2	3	4	5
28.19	Data storage procedures consider retrieval requirements, cost-effectiveness and security policy.	0	1	2	3	4	5
28.20	Retention periods and storage terms are defined for documents,	0	1	2	3	4	5

	data, programs, reports and messages (incoming and outgoing) as well as the data (keys, certificates) used for their encryption and authentication.						
28.21	Contents of the IT function's media library containing data are inventoried systematically and any discrepancies disclosed by a physical inventory are remedied in a timely fashion and measures are taken to maintain the integrity of magnetic and optical media stored in the library.	0	1	2	3	4	5
28.22	Housekeeping procedures designed to protect media library contents have been established by IT management. Standards are defined for the external identification of magnetic media and the control of their physical movement and storage to support accountability.	0	1	2	3	4	5
28.23	Management implements a proper strategy for back-up and restoration to ensure that it includes a review of business requirements, as well as the development, implementation, testing and documentation of the recovery plan. Backups satisfy the above-mentioned requirements.	0	1	2	3	4	5
28.24	Back-ups are taken in accordance with the defined back-up strategy and the usability of back-ups is regularly verified.	0	1	2	3	4	5
28.25	Back-up procedures for IT-related media include the proper storage of the data files, software and related documentation, both on-site and off-site. Back-ups are stored securely and the storage sites periodically reviewed regarding physical access security and security of data files and other items.	0	1	2	3	4	5
28.26	Data archival meets legal and business requirements, and is properly safeguarded and accounted for.	0	1	2	3	4	5
28.27	Regarding data transmission over the Internet or any other public network, management defined and implements procedures and protocols ensuring integrity, confidentiality and non-repudiation of sensitive messages.	0	1	2	3	4	5
28.28	The authentication and integrity of information originated outside the organization, whether received by telephone, voicemail, paper document, fax or e-mail, are appropriately	0	1	2	3	4	5

	checked before potentially critical action is taken.						
28.29	Taking into consideration that the traditional boundaries of time and geography are less reliant, management has defined and implements appropriate procedures and practices for sensitive and critical electronic transactions ensuring integrity and authenticity of: • atomicity (indivisible unit of work, all of its actions succeed or they all fail) • consistency (if the transaction cannot achieve a stable end state, it must return the system to its initial state) • isolation (a transaction's behavior is not affected by other transactions that execute concurrently) • durability (transaction's effects are permanent after it commits, its changes should survive system failures)	0	1	2	3	4	5
28.30	The integrity and correctness of the data kept on files and other media (e.g., electronic cards) is checked periodically. Specific attention is paid to value tokens, reference files and files containing privacy information.	0	1	2	3	4	5
28.31	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(DS12) Manage Facilities
Business Need:	Providing a suitable physical surrounding which protects the IT equipment and people against man-made and natural hazards.

#	Questions	**Response**					
29.1	Appropriate physical security and access control measures are established for IT facilities, including off-site use of information devices in conformance with the general security policy. IT resources located in public areas are appropriately protected to prevent or deter loss or damage from theft or vandalism.	0	1	2	3	4	5
29.2	A low profile is kept and the physical identification of the site of the IT operations is limited.	0	1	2	3	4	5
29.3	Individuals who are not members of the IT function's operations group are escorted by a member of that group when they must enter the computer facilities. A visitor's log is kept and reviewed regularly.	0	1	2	3	4	5
29.4	Health and safety practices are in place and maintained in conformance with applicable international, national, regional, state and local laws and regulations.	0	1	2	3	4	5
29.5	Sufficient measures are in place and maintained for protection against environmental factors (e.g., fire, dust, power, excessive heat and humidity). Specialized equipment and devices to monitor and control the environment is installed.	0	1	2	3	4	5
29.6	Management regularly assesses the need for uninterruptible power supply batteries and generators for critical IT applications to secure against power failures and fluctuations. When justified, the most appropriate equipment is installed.	0	1	2	3	4	5
29.7	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(DS13) Manage Operations						
Business Need:	Important IT support functions are performed regularly and in an orderly fashion.						
#	**Questions**	**Response**					
30.1	All IT solutions and platforms in place are operated using standard and documented procedures, which are reviewed periodically to ensure effectiveness and adherence.	0	1	2	3	4	5
30.2	The operations staff is adequately familiar and confident with the start-up process and other operations tasks by having them documented, periodically tested and adjusted when required.	0	1	2	3	4	5
30.3	The continuous scheduling of jobs, processes and tasks is organized into the most efficient sequence, maximizing throughput and utilization, to meet the objectives set in service level agreements.	0	1	2	3	4	5
30.4	Procedures are in place to identify, investigate and approve departures from standard job schedules.	0	1	2	3	4	5
30.5	Procedures require processing continuity during operator shift changes by providing for formal handover of activity, status updates and reports on current responsibilities.	0	1	2	3	4	5
30.6	Sufficient chronological information is being stored in operations logs to enable the reconstruction, review and examination of the time sequences of processing and the other activities surrounding or supporting processing.	0	1	2	3	4	5
30.7	Appropriate physical safeguards exist over special forms, such as negotiable instruments, and over sensitive output devices, such as signature cartridges, taking into consideration proper accounting of IT resources, forms or items requiring additional protection and inventory management.	0	1	2	3	4	5
30.8	For remote operations, specific procedures ensure that the connection and disconnection of the links to the remote site(s) are defined and implemented.	0	1	2	3	4	5
30.9	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(M1) Monitor the process						
Business Need:	To ensure the achievement of the performance objectives set for the IT processes.						
#	**Questions**	**Response**					
31.1	Relevant performance indicators (e.g., benchmarks) from both internal and external sources are defined and data is being collected for the creation of management information reports and exception reports regarding these indicators.	0	1	2	3	4	5
31.2	Services delivered by the IT function are measured (key performance indicators and/or critical success factors) by management and compared with target levels on a continuous basis.	0	1	2	3	4	5
31.3	At regular intervals, management measures customer satisfaction regarding the services delivered by the IT function and identifies shortfalls in service levels and establishes improvement objectives.	0	1	2	3	4	5
31.4	Management reports are provided for senior management's review of the organization's progress toward identified goals. Status reports include the extent to which planned objectives have been achieved, deliverables obtained, performance targets met and risks mitigated.	0	1	2	3	4	5
31.5	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(M2) Assess internal control adequacy						
Business Need:	To ensure the achievement of the internal control objectives set for the IT processes.						
#	**Questions**	**Response**					
32.1	Management regularly monitors the effectiveness of internal controls in the normal course of operations through management and supervisory activities, comparisons, reconciliations and other routine actions. Deviations evoke analysis and corrective action.	0	1	2	3	4	5
32.2	Information regarding errors, inconsistencies and exceptions should be kept and systematically reported to management.	0	1	2	3	4	5
32.3	Management reports information on internal control levels and exceptions to the affected parties to ensure the continued effectiveness of its internal control system.	0	1	2	3	4	5

32.4	Operational security and internal controls are regularly evaluated against the requirements. Ongoing monitoring activities look for vulnerabilities and security problems.	0	1	2	3	4	5
32.5	How relevant is this IT process to your organization?	0	1	2	3	4	5

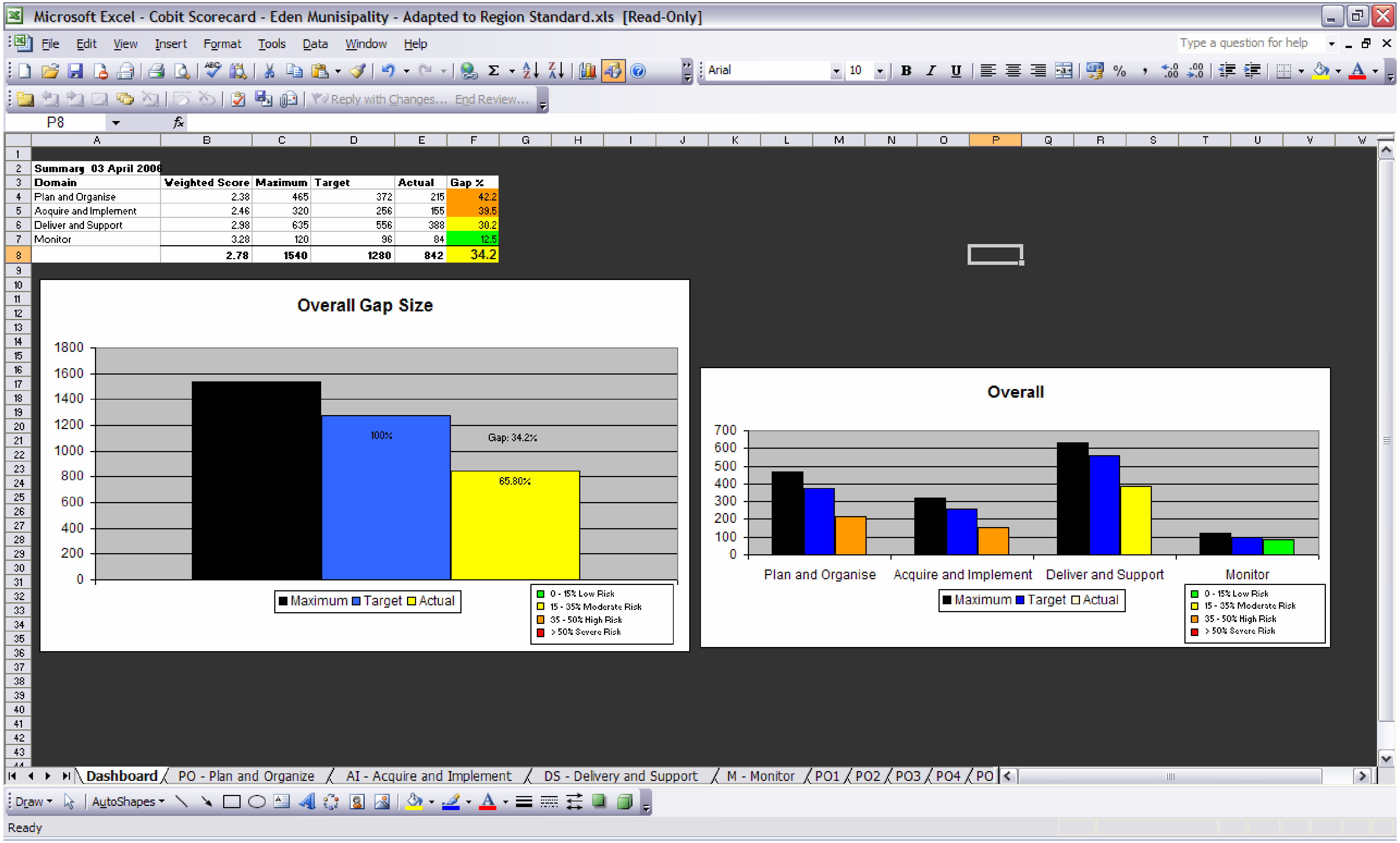
Business Process:	(M3) Obtain independent assurance						
Business Need:	To increase confidence and trust among the organization, customers, and third-party providers						
#	**Questions**	**Response**					
33.1	Management obtains independent certification/accreditation of security and internal controls prior to implementing critical new IT services and re-certify or re-accreditate these services on a routine cycle after implementation.	0	1	2	3	4	5
33.2	Management obtains independent certification/accreditation of security and internal controls prior to using IT service providers and re-certify/re-accreditate on a routine cycle.	0	1	2	3	4	5
33.3	Management obtains independent evaluation of the effectiveness of IT services on a routine cycle.	0	1	2	3	4	5
33.4	Management obtains independent evaluation of the effectiveness of IT service providers on a routine cycle.	0	1	2	3	4	5
33.5	Management obtains independent assurance of the IT function's compliance with legal and regulatory requirements, and contractual commitments on a routine cycle.	0	1	2	3	4	5
33.6	Management obtains independent assurance of third-party service providers' compliance with legal and regulatory requirements and contractual commitments on a routine cycle.	0	1	2	3	4	5
33.7	The independent assurance function possesses the technical competence, and skills and knowledge necessary to perform such reviews in an effective, efficient and economical manner.	0	1	2	3	4	5
33.8	IT management seeks audit involvement in a proactive manner before finalizing IT service solutions.	0	1	2	3	4	5
33.9	How relevant is this IT process to your organization?	0	1	2	3	4	5

Business Process:	(M4) Provide for independent audit
Business Need:	To increase confidence levels and benefit from best practice advice

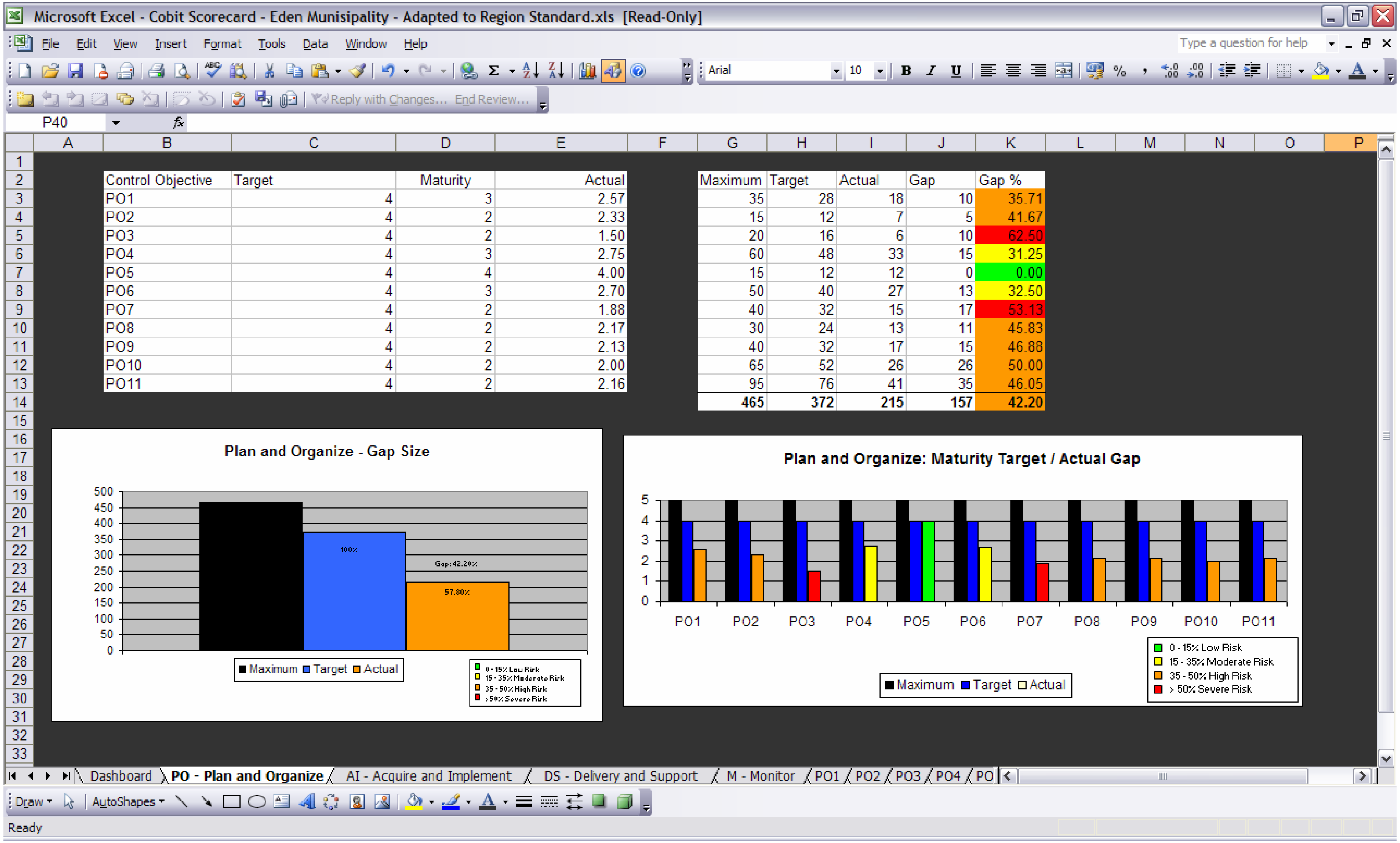
#	**Questions**	**Response**					
34.1	An audit charter document, defined by senior management, is established and outlines the responsibility, authority and accountability of the audit function. The charter is reviewed periodically to assure that the independence, authority and accountability of the audit function are maintained.	0	1	2	3	4	5
34.2	Auditors are external to the department/function being audited, preferably external from the organization	0	1	2	3	4	5
34.3	The audit function adheres to codes of professional ethics and auditing standards. Due professional care should is exercised in all aspects of the audit work, including the observance of applicable audit and IT standards.	0	1	2	3	4	5
34.4	The auditors responsible for the review of the organization's IT activities are technically competent and collectively possess the skills and knowledge (i.e., CISA domains) necessary to perform such reviews in an effective, efficient and economical manner.	0	1	2	3	4	5
34.5	Regular and independent audits are obtained regarding the effectiveness, efficiency and economy of security and internal control procedures, and management's ability to control IT function activities.	0	1	2	3	4	5
34.6	Audits are appropriately supervised to provide assurances that audit objectives are achieved and applicable professional auditing standards are met.	0	1	2	3	4	5
34.7	The audit function provides a report, in an appropriate form, to intended recipients upon the completion of audit work. The audit report states the scope and objectives of the audit, the period of coverage, and the nature and extent of the audit work performed.	0	1	2	3	4	5
34.8	Auditors can request and evaluate appropriate information on previous findings, conclusions and recommendations to determine whether appropriate actions have been implemented in a timely manner.	0	1	2	3	4	5
34.9	How relevant is this IT process to your organization?	0	1	2	3	4	5

Appendix B

COBIT Gap Analysis Tool



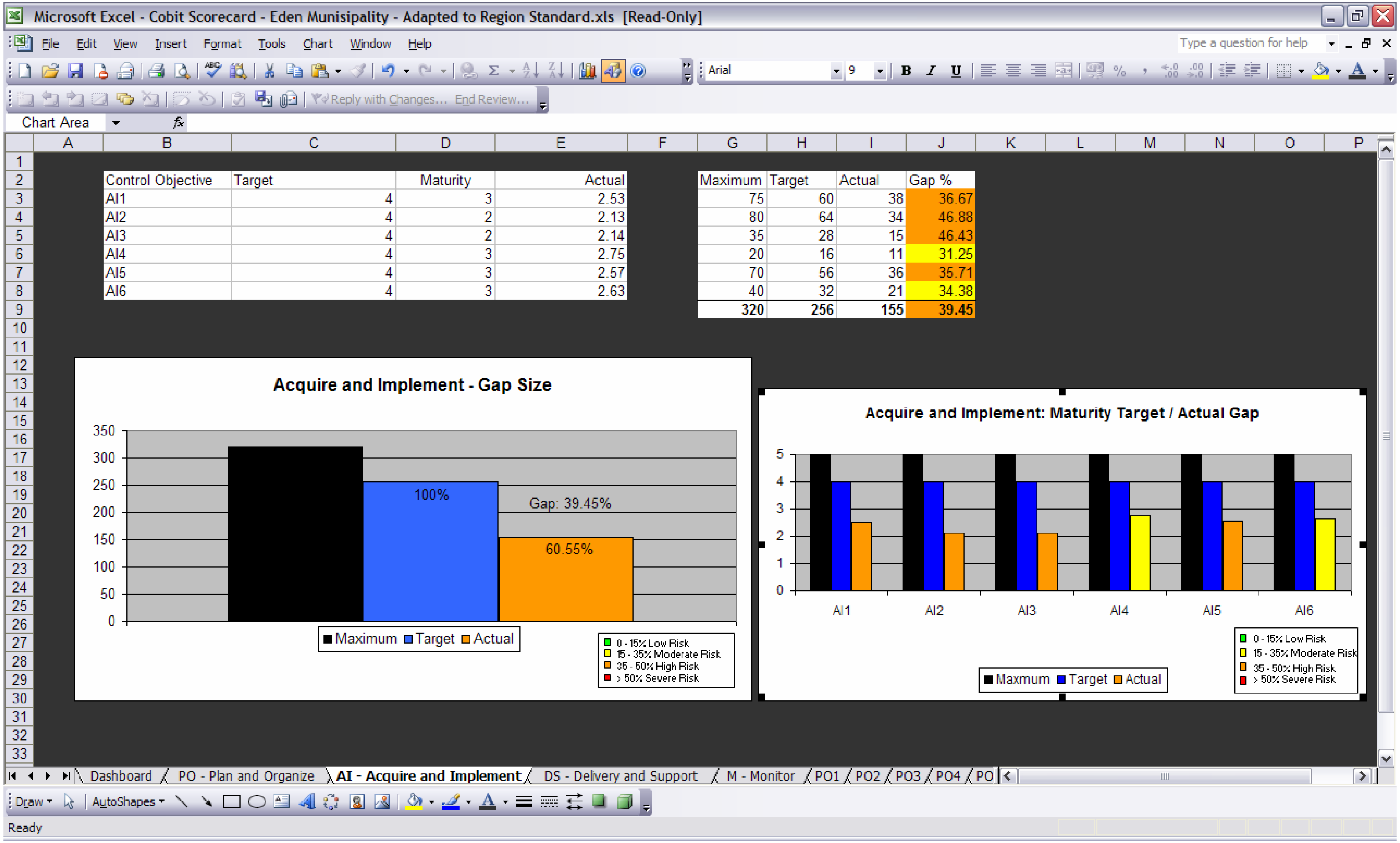
Summary 03 April 2006					
Domain	Weighted Score	Maximum	Target	Actual	Gap %
Plan and Organise	2.38	465	372	215	42.2
Acquire and Implement	2.46	320	256	155	39.5
Deliver and Support	2.98	635	556	388	30.2
Monitor	3.28	120	96	84	12.5
	2.78	1540	1280	842	34.2



Microsoft Excel - Cobit Scorecard - Eden Munisipality - Adapted to Region Standard.xls [Read-Only]

Control Objective	Target	Maturity	Actual
PO1	4	3	2.57
PO2	4	2	2.33
PO3	4	2	1.50
PO4	4	3	2.75
PO5	4	4	4.00
PO6	4	3	2.70
PO7	4	2	1.88
PO8	4	2	2.17
PO9	4	2	2.13
PO10	4	2	2.00
PO11	4	2	2.16

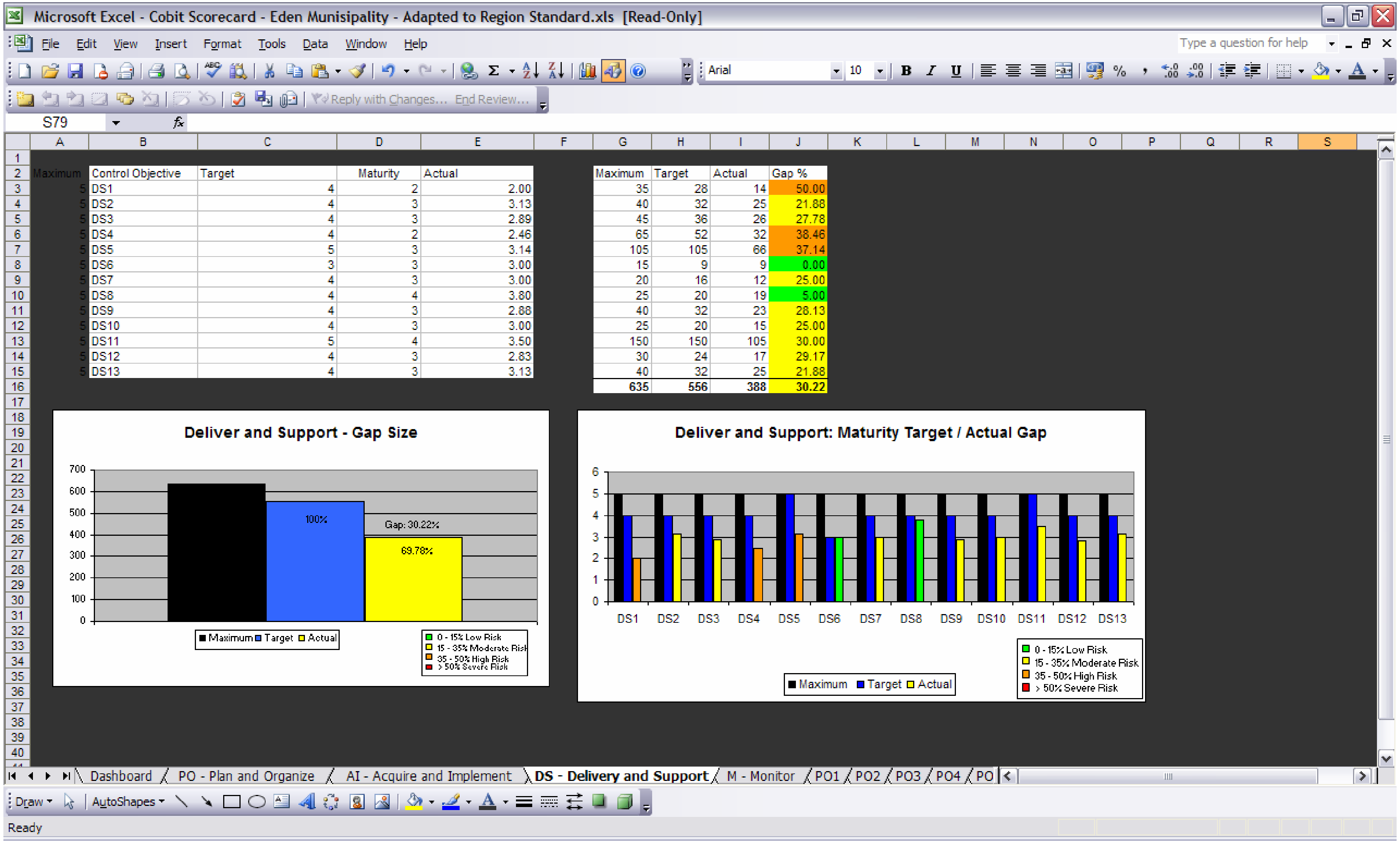
Maximum	Target	Actual	Gap	Gap %
35	28	18	10	35.71
15	12	7	5	41.67
20	16	6	10	62.50
60	48	33	15	31.25
15	12	12	0	0.00
50	40	27	13	32.50
40	32	15	17	53.13
30	24	13	11	45.83
40	32	17	15	46.88
65	52	26	26	50.00
95	76	41	35	46.05
465	**372**	**215**	**157**	**42.20**


Microsoft Excel - Cobit Scorecard - Eden Munisipality - Adapted to Region Standard.xls [Read-Only]
File Edit View Insert Format Tools Chart Window Help
Type a question for help
Arial 9
Reply with Changes... End Review...
Chart Area
Dashboard
PO - Plan and Organize
AI - Acquire and Implement
DS - Delivery and Support
M - Monitor
PO1
PO2
PO3
PO4
PO
Draw
AutoShapes
Ready

Control Objective	Target	Maturity	Actual
AI1	4	3	2.53
AI2	4	2	2.13
AI3	4	2	2.14
AI4	4	3	2.75
AI5	4	3	2.57
AI6	4	3	2.63

Maximum	Target	Actual	Gap %
75	60	38	36.67
80	64	34	46.88
35	28	15	46.43
20	16	11	31.25
70	56	36	35.71
40	32	21	34.38
320	256	155	39.45

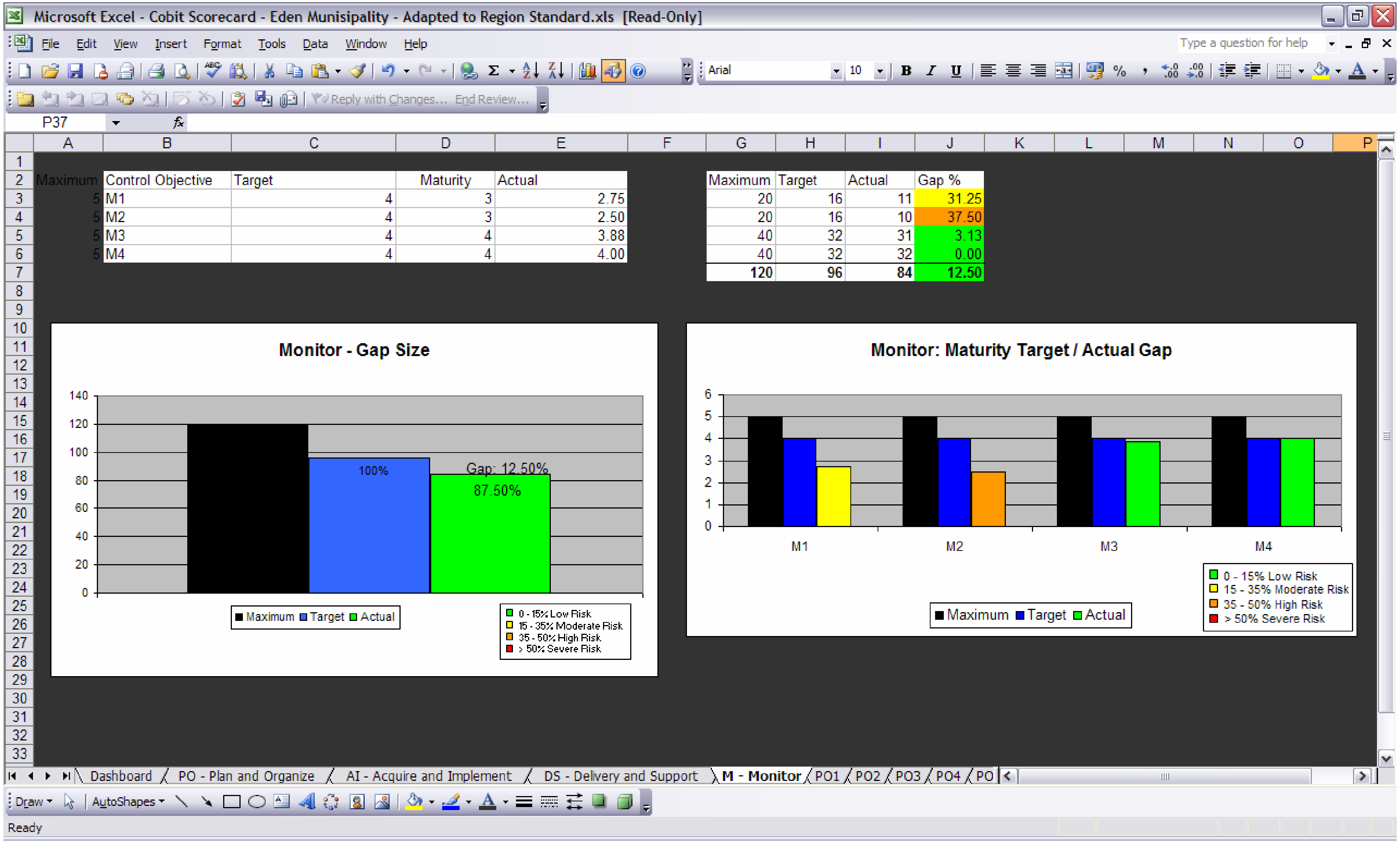
Acquire and Implement - Gap Size
350
300
250
200
150
100
50
0
100%
Gap: 39.45%
60.55%
■ Maximum ■ Target ■ Actual
🟩 0 - 15% Low Risk
🟨 15 - 35% Moderate Risk
🟧 35 - 50% High Risk
🟥 > 50% Severe Risk
Acquire and Implement: Maturity Target / Actual Gap
5
4
3
2
1
0
AI1
AI2
AI3
AI4
AI5
AI6
■ Maxmum ■ Target ■ Actual
🟩 0 - 15% Low Risk
🟨 15 - 35% Moderate Risk
🟧 35 - 50% High Risk
🟥 > 50% Severe Risk



Microsoft Excel - Cobit Scorecard - Eden Munisipality - Adapted to Region Standard.xls [Read-Only]
File Edit View Insert Format Tools Data Window Help
Type a question for help
Arial 10
Reply with Changes... End Review...
S79
Dashboard / PO - Plan and Organize / AI - Acquire and Implement / DS - Delivery and Support / M - Monitor / PO1 / PO2 / PO3 / PO4 / PO
Draw AutoShapes
Ready

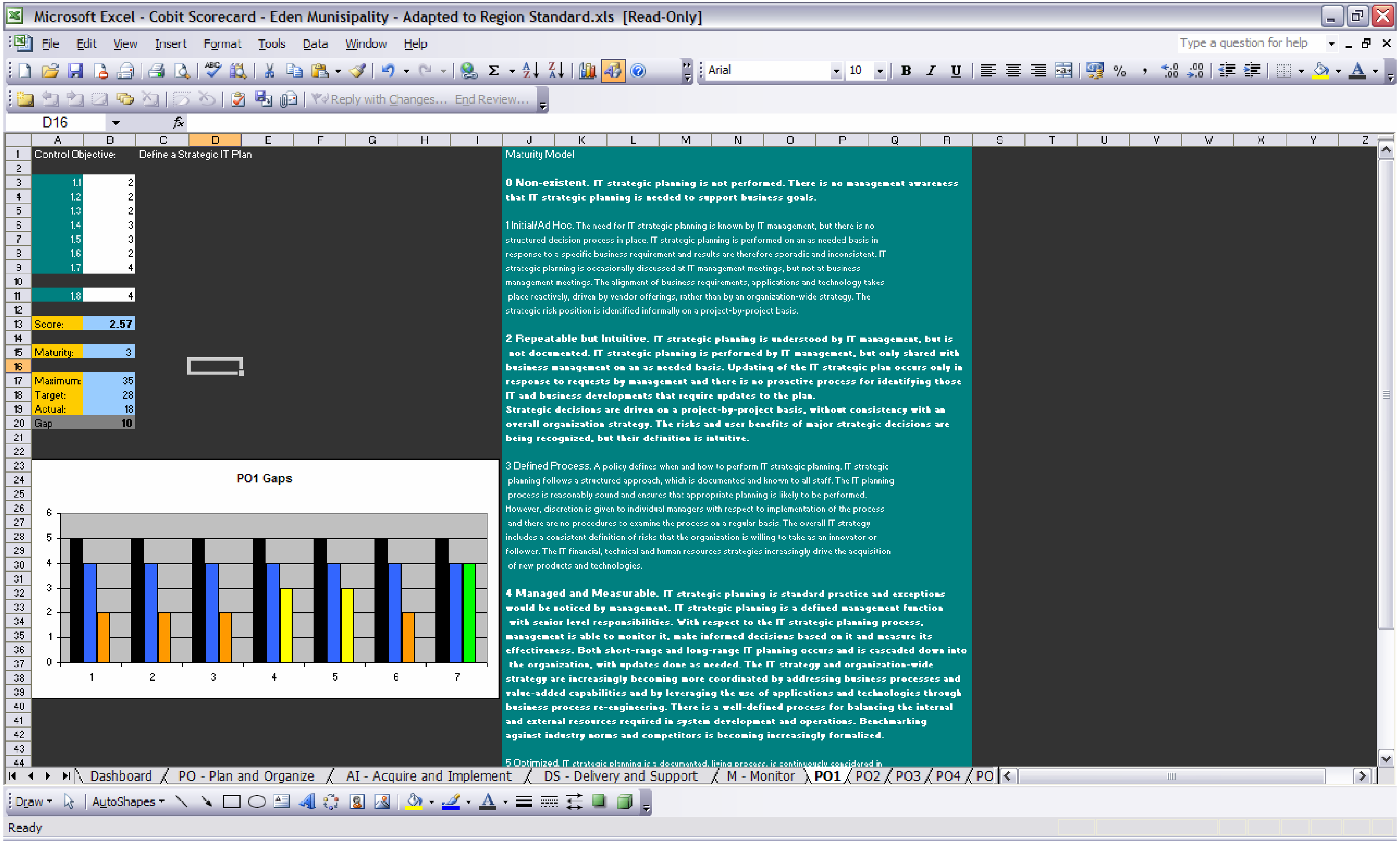
Maximum	Control Objective	Target	Maturity	Actual
5	DS1	4	2	2.00
5	DS2	4	3	3.13
5	DS3	4	3	2.89
5	DS4	4	2	2.46
5	DS5	5	3	3.14
5	DS6	3	3	3.00
5	DS7	4	3	3.00
5	DS8	4	4	3.80
5	DS9	4	3	2.88
5	DS10	4	3	3.00
5	DS11	5	4	3.50
5	DS12	4	3	2.83
5	DS13	4	3	3.13

Maximum	Target	Actual	Gap %
35	28	14	50.00
40	32	25	21.88
45	36	26	27.78
65	52	32	38.46
105	105	66	37.14
15	9	9	0.00
20	16	12	25.00
25	20	19	5.00
40	32	23	28.13
25	20	15	25.00
150	150	105	30.00
30	24	17	29.17
40	32	25	21.88
635	556	388	30.22



Maximum	Control Objective	Target	Maturity	Actual
5	M1	4	3	2.75
5	M2	4	3	2.50
5	M3	4	4	3.88
5	M4	4	4	4.00

Maximum	Target	Actual	Gap %
20	16	11	31.25
20	16	10	37.50
40	32	31	3.13
40	32	32	0.00
120	**96**	**84**	**12.50**


Microsoft Excel - Cobit Scorecard - Eden Munisipality - Adapted to Region Standard.xls [Read-Only]
File Edit View Insert Format Tools Data Window Help
Type a question for help
Arial 10
Reply with Changes... End Review...
D16
Dashboard / PO - Plan and Organize / AI - Acquire and Implement / DS - Delivery and Support / M - Monitor / PO1 / PO2 / PO3 / PO4 / PO
Draw AutoShapes
Ready
PO1 Gaps
0
1
2
3
4
5
6
1
2
3
4
5
6
7

Control Objective:		Define a Strategic IT Plan
1.1	2	
1.2	2	
1.3	2	
1.4	3	
1.5	3	
1.6	2	
1.7	4	
1.8	4	
Score:	2.57	
Maturity:	3	
Maximum:	35	
Target:	28	
Actual:	18	
Gap	10	

Maturity Model

0 Non-existent. IT strategic planning is not performed. There is no management awareness that IT strategic planning is needed to support business goals.

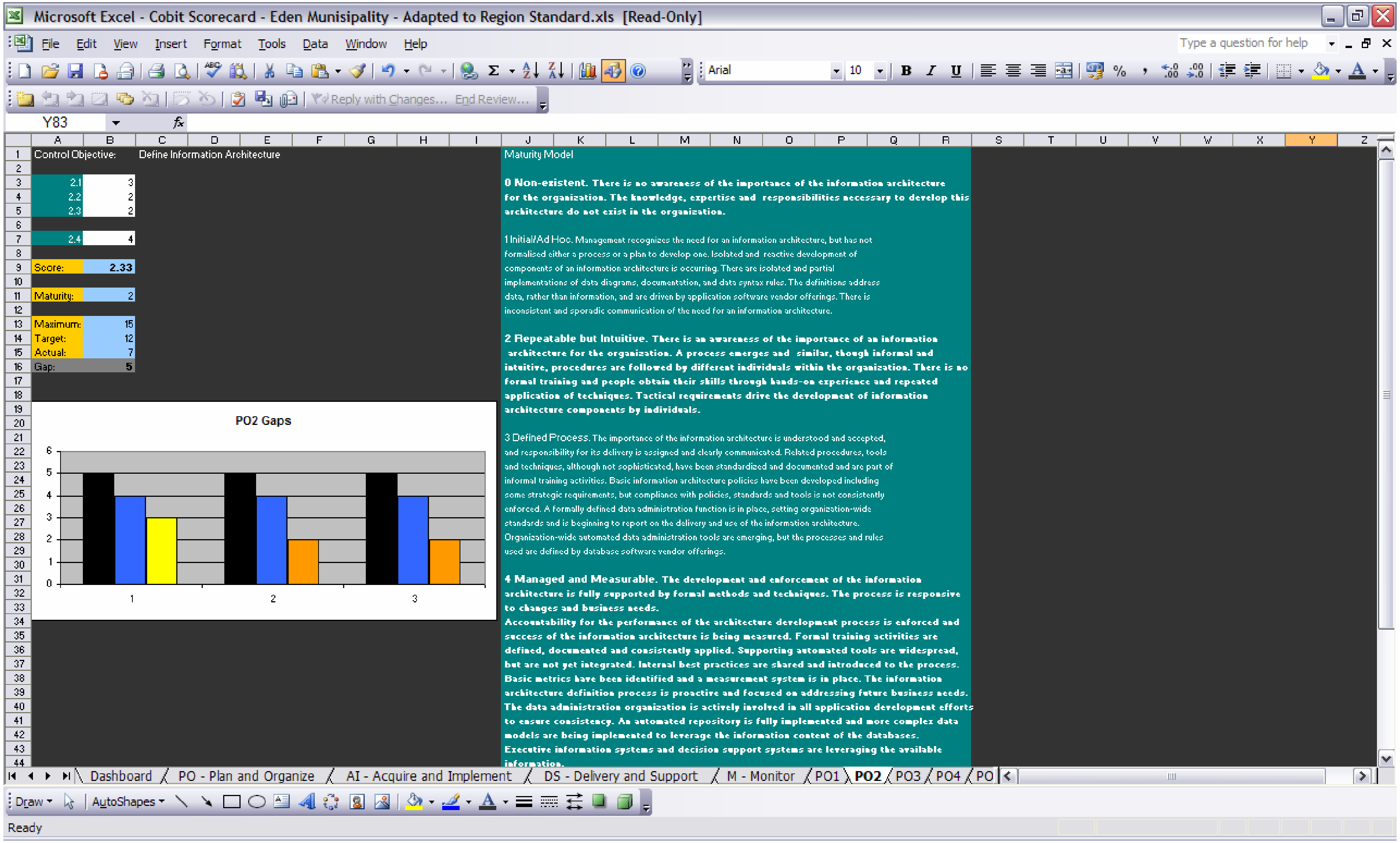
1 Initial/Ad Hoc. The need for IT strategic planning is known by IT management, but there is no structured decision process in place. IT strategic planning is performed on an as needed basis in response to a specific business requirement and results are therefore sporadic and inconsistent. IT strategic planning is occasionally discussed at IT management meetings, but not at business management meetings. The alignment of business requirements, applications and technology takes place reactively, driven by vendor offerings, rather than by an organization-wide strategy. The strategic risk position is identified informally on a project-by-project basis.

2 Repeatable but Intuitive. IT strategic planning is understood by IT management, but is not documented. IT strategic planning is performed by IT management, but only shared with business management on an as needed basis. Updating of the IT strategic plan occurs only in response to requests by management and there is no proactive process for identifying those IT and business developments that require updates to the plan.
Strategic decisions are driven on a project-by-project basis, without consistency with an overall organization strategy. The risks and user benefits of major strategic decisions are being recognized, but their definition is intuitive.

3 Defined Process. A policy defines when and how to perform IT strategic planning. IT strategic planning follows a structured approach, which 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 on a regular basis. The overall IT strategy includes a consistent definition of risks that the organization is willing to take as an innovator or follower. The IT financial, technical and human resources strategies increasingly drive the acquisition of new products and technologies.

4 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. With respect to the IT strategic planning process, management is able to monitor it, 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 organization, with updates done as needed. The IT strategy and organization-wide strategy are increasingly becoming more coordinated by addressing business processes and value-added capabilities and by leveraging the use of applications and technologies through business process re-engineering. There is a well-defined process for balancing the internal and external resources required in system development and operations. Benchmarking against industry norms and competitors is becoming increasingly formalized.

5 Optimized. IT strategic planning is a documented, living process, is continuously considered in


Microsoft Excel - Cobit Scorecard - Eden Munisipality - Adapted to Region Standard.xls [Read-Only]
File Edit View Insert Format Tools Data Window Help
Type a question for help
Arial
10
Reply with Changes... End Review...
Y83
PO2 Gaps
6
5
4
3
2
1
0
1
2
3
Dashboard
PO - Plan and Organize
AI - Acquire and Implement
DS - Delivery and Support
M - Monitor
PO1
PO2
PO3
PO4
PO
Draw
AutoShapes
Ready

Control Objective: Define Information Architecture

2.1	3
2.2	2
2.3	2
2.4	4
Score:	2.33
Maturity:	2
Maximum:	15
Target:	12
Actual:	7
Gap:	5

Maturity Model

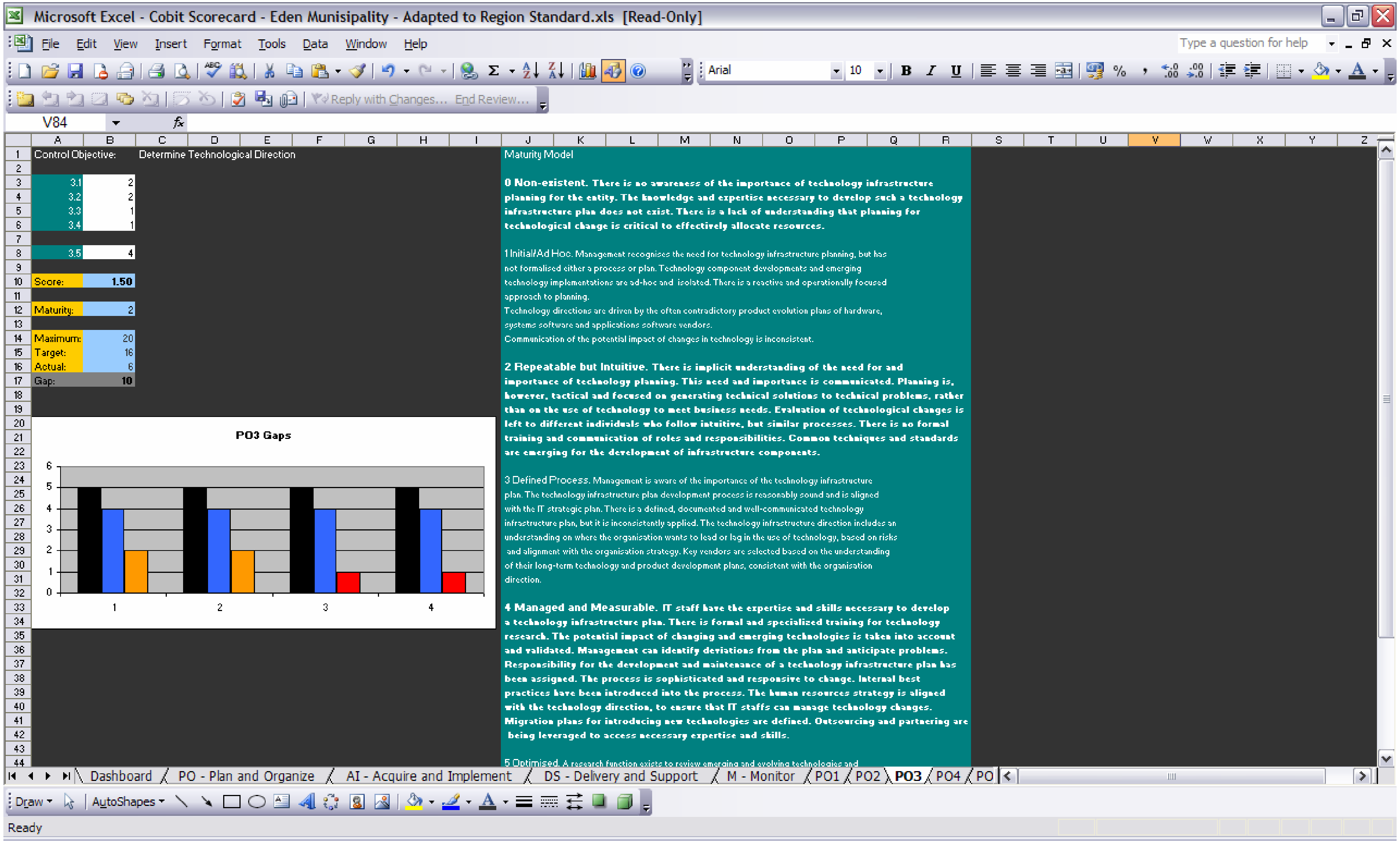
0 Non-existent. There is no awareness of the importance of the information architecture for the organization. The knowledge, expertise and responsibilities necessary to develop this architecture do not exist in the organization.

1 Initial/Ad Hoc. Management recognizes the need for an information architecture, but has not formalised either a process or a plan to develop one. Isolated and reactive development of components of an information architecture is occurring. There are isolated and partial implementations of data diagrams, documentation, and data syntax rules. The definitions address data, rather than information, and are driven by application software vendor offerings. There is inconsistent and sporadic communication of the need for an information architecture.

2 Repeatable but Intuitive. There is an awareness of the importance of an information architecture for the organization. A process emerges and similar, though informal and intuitive, procedures are followed by different individuals within the organization. There is no formal training and people obtain their skills through hands-on experience and repeated application of techniques. Tactical requirements drive the development of information architecture components by individuals.

3 Defined Process. The importance of the information architecture is understood and accepted, and responsibility for its delivery is assigned and clearly communicated. Related procedures, tools and techniques, although not sophisticated, have been standardized and documented and are part of informal training activities. Basic information architecture policies have been developed including some strategic requirements, but compliance with policies, standards and tools is not consistently enforced. A formally defined data administration function is in place, setting organization-wide standards and is beginning to report on the delivery and use of the information architecture. Organization-wide automated data administration tools are emerging, but the processes and rules used are defined by database software vendor offerings.

4 Managed and Measurable. The development and enforcement of the information architecture is fully supported by formal methods and techniques. The process is responsive to changes and business needs. Accountability for the performance of the architecture development process is enforced and success of the information architecture is being measured. Formal training activities are defined, documented and consistently applied. Supporting automated tools are widespread, but are not yet integrated. Internal best practices are shared and introduced to the process. Basic metrics have been identified and a measurement system is in place. The information architecture definition process is proactive and focused on addressing future business needs. The data administration organization is actively involved in all application development efforts to ensure consistency. An automated repository is fully implemented and more complex data models are being implemented to leverage the information content of the databases. Executive information systems and decision support systems are leveraging the available information.



Microsoft Excel - Cobit Scorecard - Eden Munisipality - Adapted to Region Standard.xls [Read-Only]

Control Objective:	Determine Technological Direction
3.1	2
3.2	2
3.3	1
3.4	1
3.5	4
Score:	1.50
Maturity:	2
Maximum:	20
Target:	16
Actual:	6
Gap:	10

PO3 Gaps

Maturity Model

0 Non-existent. There is no awareness of the importance of technology infrastructure planning for the entity. The knowledge and expertise necessary to develop such a technology infrastructure plan does not exist. There is a lack of understanding that planning for technological change is critical to effectively allocate resources.

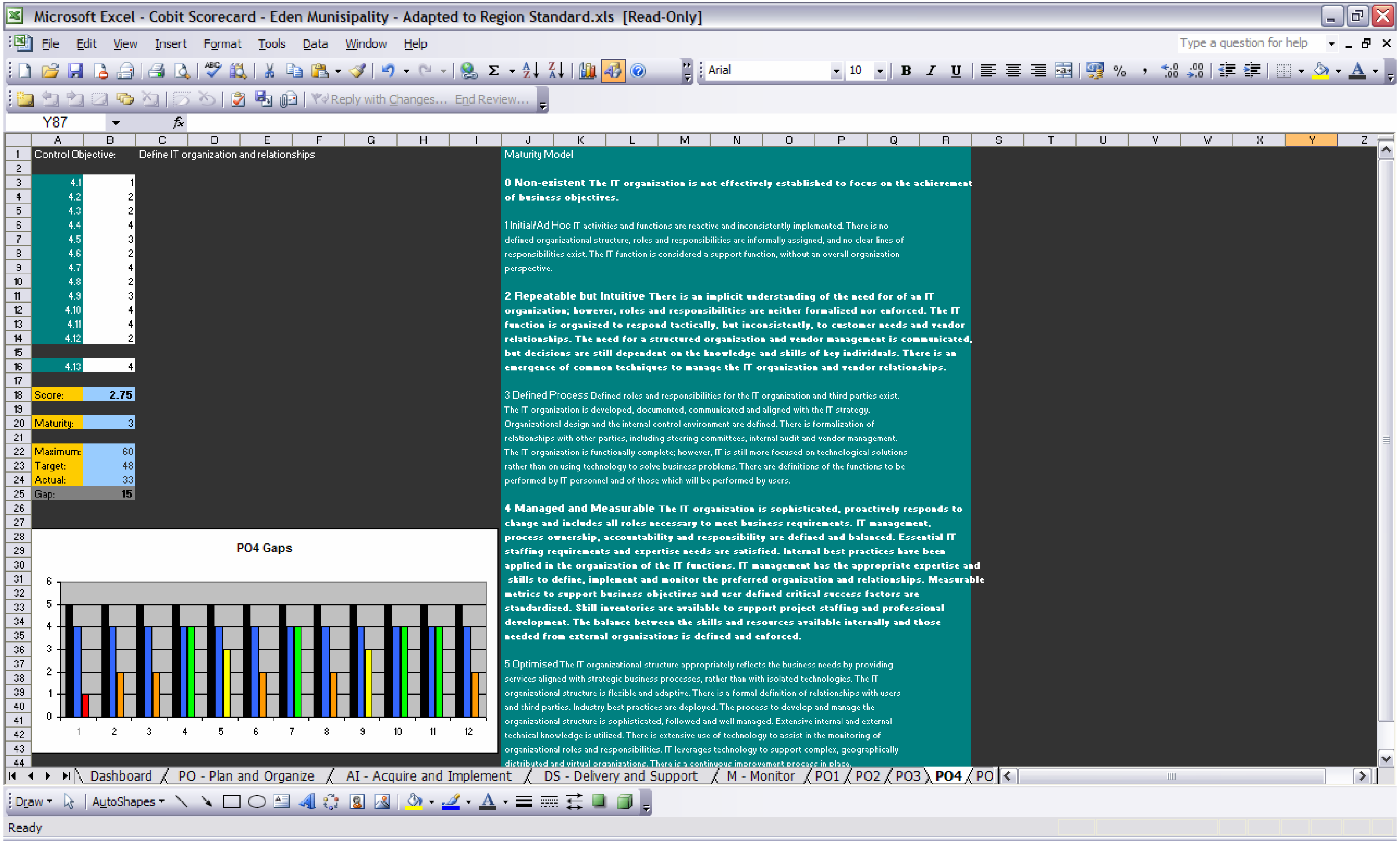
1 Initial/Ad Hoc. Management recognises the need for technology infrastructure planning, but has not formalised either a process or plan. Technology component developments and emerging technology implementations are ad-hoc and isolated. There is a reactive and operationally focused approach to planning.
Technology directions are driven by the often contradictory product evolution plans of hardware, systems software and applications software vendors.
Communication of the potential impact of changes in technology is inconsistent.

2 Repeatable but Intuitive. There is implicit understanding of the need for and importance of technology planning. This need and importance is communicated. Planning is, however, tactical and focused on generating technical solutions to technical problems, rather than on the use of technology to meet business needs. Evaluation of technological changes is left to different individuals who follow intuitive, but similar processes. There is no formal training and communication of roles and responsibilities. Common techniques and standards are emerging for the development of infrastructure components.

3 Defined Process. Management is aware of the importance of the technology infrastructure plan. The technology infrastructure plan development process is reasonably sound and is aligned with the IT strategic plan. There is a defined, documented and well-communicated technology infrastructure plan, but it is inconsistently applied. The technology infrastructure direction includes an understanding on where the organisation wants to lead or lag in the use of technology, based on risks and alignment with the organisation strategy. Key vendors are selected based on the understanding of their long-term technology and product development plans, consistent with the organisation direction.

4 Managed and Measurable. IT staff have the expertise and skills necessary to develop a technology infrastructure plan. There is formal and specialized training for technology research. The potential impact of changing and emerging technologies is taken into account and validated. Management can identify deviations from the plan and anticipate problems. Responsibility for the development and maintenance of a technology infrastructure plan has been assigned. The process is sophisticated and responsive to change. Internal best practices have been introduced into the process. The human resources strategy is aligned with the technology direction, to ensure that IT staffs can manage technology changes. Migration plans for introducing new technologies are defined. Outsourcing and partnering are being leveraged to access necessary expertise and skills.

5 Optimised. A research function exists to review emerging and evolving technologies and



Microsoft Excel - Cobit Scorecard - Eden Munisipality - Adapted to Region Standard.xls [Read-Only]
File Edit View Insert Format Tools Data Window Help
Type a question for help
Arial 10
Reply with Changes... End Review...
Y87
Dashboard / PO - Plan and Organize / AI - Acquire and Implement / DS - Delivery and Support / M - Monitor / PO1 / PO2 / PO3 / PO4 / PO
Draw AutoShapes
Ready

Control Objective: Define IT organization and relationships

4.1	1
4.2	2
4.3	2
4.4	4
4.5	3
4.6	2
4.7	4
4.8	2
4.9	3
4.10	4
4.11	4
4.12	2
4.13	4
Score:	2.75
Maturity:	3
Maximum:	60
Target:	48
Actual:	33
Gap:	15

PO4 Gaps

6
5
4
3
2
1
0
1
2
3
4
5
6
7
8
9
10
11
12

Maturity Model

0 Non-existent The IT organization is not effectively established to focus on the achievement of business objectives.

1 Initial/Ad Hoc IT activities and functions are reactive and inconsistently implemented. There is no defined organizational structure, roles and responsibilities are informally assigned, and no clear lines of responsibilities exist. The IT function is considered a support function, without an overall organization perspective.

2 Repeatable but Intuitive There is an implicit understanding of the need for of an IT organization; however, roles and responsibilities are neither formalized nor enforced. The IT function is organized to respond tactically, but inconsistently, to customer needs and vendor relationships. The need for a structured organization and vendor management is communicated, but decisions are still dependent on the knowledge and skills of key individuals. There is an emergence of common techniques to manage the IT organization and vendor relationships.

3 Defined Process Defined roles and responsibilities for the IT organization and third parties exist. The IT organization is developed, documented, communicated and aligned with the IT strategy. Organizational design and the internal control environment are defined. There is formalization of relationships with other parties, including steering committees, internal audit and vendor management. The IT organization is functionally complete; however, IT is still more focused on technological solutions rather than on using technology to solve business problems. There are definitions of the functions to be performed by IT personnel and of those which will be performed by users.

4 Managed and Measurable The IT organization is sophisticated, proactively responds to change and includes all roles necessary to meet business requirements. IT management, process ownership, accountability and responsibility are defined and balanced. Essential IT staffing requirements and expertise needs are satisfied. Internal best practices have been applied in the organization of the IT functions. IT management has the appropriate expertise and skills to define, implement and monitor the preferred organization and relationships. Measurable metrics to support business objectives and user defined critical success factors are standardized. Skill inventories are available to support project staffing and professional development. The balance between the skills and resources available internally and those needed from external organizations is defined and enforced.

5 Optimised The IT organizational structure appropriately reflects the business needs by providing services aligned with strategic business processes, rather than with isolated technologies. The IT organizational structure is flexible and adaptive. There is a formal definition of relationships with users and third parties. Industry best practices are deployed. The process to develop and manage the organizational structure is sophisticated, followed and well managed. Extensive internal and external technical knowledge is utilized. There is extensive use of technology to assist in the monitoring of organizational roles and responsibilities. IT leverages technology to support complex, geographically distributed and virtual organizations. There is a continuous improvement process in place.

This appendix contains the screenshots from the tool that is representative of the various levels within COBIT, Dashboard, four COBIT domains and four high-level control objectives from the Plan and Organise domain, PO1, PO2, PO3 and PO4. The other 30 high-level control objectives have the same look and functionality as the above screenshots. PO1 to PO4 provide sufficient information and no new information would be gained if the other 30 objectives' screens were also added.

Appendix C

ISO 17799 Analysis Questionnaire

The size of this questionnaire is over 100 pages and therefore only a part of it has been added as an appendix.

9 Physical and environmental security

9.1 Secure areas

9.1.1 Physical security perimeter

Control

Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.

Question	Yes	Partially	No	Comments
Security perimeters are clearly defined with the placement and strength of the security controls depending of the requirements from the assets within the perimeter.				
Building perimeters are secure with no gaps for access. Solid walls, security locks on doors etc				
A manned reception area exist				
Access to sites and buildings are restricted to authorised personnel.				
Physical barriers have been built to prevent unauthorized physical access and environmental contamination				
all fire doors on a security perimeter are alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance				
suitable intruder detection systems have been installed				
information processing facilities managed by the organization are physically separated from those managed by third parties.				

9.1.2 Physical entry controls

Control

Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Question	Yes	Partially	No	Comments
For visitors, the date and time of entry and departure are recorded				
access to areas where sensitive information is processed or stored should be controlled and restricted to authorized persons only;				
all employees, contractors and third party users and all visitors are required to wear some form of visible identification and would immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;				
third party support service personnel is granted restricted access to secure areas or sensitive information processing facilities only when required;				
access rights to secure areas are regularly reviewed and updated				

9.1.3 Securing offices, rooms, and facilities

Control

Physical security for offices, rooms, and facilities should be designed and applied.

Question	Yes	Partially	No	Comments
key facilities are located in specific areas to avoid access by the public				
where applicable, buildings or rooms are unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities;				

9.1.4 Protecting against external and environmental threats

Control
Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.

Question	Yes	Partially	No	Comments
Hazardous or combustible materials should be stored at a safe distance from a secure area. Bulk supplies such as stationery should not be stored within a secure area;				
fallback equipment and back-up media should be sited at a safe distance to avoid damage from a disaster affecting the main site;				
Appropriate fire fighting equipment should be provided and suitably placed.				

9.1.5 Working in secure areas

Control
Physical protection and guidelines for working in secure areas should be designed and applied.

Question	Yes	Partially	No	Comments
personnel should only be aware of the existence of, or activities within, a secure area on a need to know basis;				
unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities;				
vacant secure areas should be physically locked and periodically checked;				
photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorized;				

9.1.6 Public access, delivery, and loading areas

Control

Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

Question	Yes	Partially	No	Comments
access to a delivery and loading area from outside of the building are restricted to identified and authorized personnel;				
the delivery and loading area is designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building;				
the external doors of a delivery and loading area should be secured when the internal doors are opened;				
incoming material should be inspected for potential threats before this material is moved from the delivery and loading area to the point of use;				
Incoming material should be registered in accordance with asset management procedures on entry to the site;				
Incoming and outgoing shipments should be physically segregated, where possible.				

*If **Partially** or **No** were answers to any of the above questions, tick the relevant constraints in the corresponding boxes below:*

Control	Risk	Budget	Environ-ment	Tech-nology	Culture	Time	Not Applicable	Other
9.1.1								
9.1.2								
9.1.3								
9.1.4								
9.1.5								
9.1.6								

9.2 Equipment security

9.2.1 Equipment siting and protection management

Control

Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Question	Yes	Partially	No	Comments
equipment should be sited to minimize unnecessary access into work areas;				
information processing facilities handling sensitive data should be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons during their use, and storage facilities secured to avoid unauthorized access;				
items requiring special protection should be isolated to reduce the general level of protection required;				
controls should be adopted to minimize the risk of potential physical threats				
guidelines for eating, drinking, and smoking in proximity to information processing facilities should be established;				
environmental conditions, such as temperature and humidity, should be monitored for conditions, which could adversely affect the operation of information processing facilities				
lightning protection should be applied to all buildings and lightning protection filters should be fitted to all incoming power and communications lines;				
the use of special protection methods, such as keyboard membranes, should be considered for equipment in industrial environments;				

9.2.2 Supporting utilities management

Control

Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.

Question	Yes	Partially	No	Comments
All supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning should be adequate for the systems they are supporting. Support utilities should be regularly inspected and as appropriate tested to ensure their proper functioning and to reduce any risk from their malfunction or failure				
An uninterruptible power supply (UPS) to support orderly close down or continuous running is recommended for equipment supporting critical business operations. Power contingency plans should cover the action to be taken on failure of the UPS				
A back-up generator should be considered if processing is required to continue in case of a prolonged power failure.				
An adequate supply of fuel should be available to ensure that the generator can perform for a prolonged period.				
UPS equipment and generators should be regularly checked to ensure it has adequate capacity and is tested in accordance with the manufacturer's recommendations.				
Emergency power off switches should be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. Emergency lighting should be provided in case of main power failure.				
The water supply should be stable and adequate to supply air conditioning, humidification equipment and fire suppression systems (where used)				
Telecommunications equipment				

should be connected to the utility provider by at least two diverse routes to prevent failure in one connection path removing voice services.				

9.2.3 Cabling security time, management

Control

Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.

Question	Yes	Partially	No	Comments
power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection;				
network cabling should be protected from unauthorized interception or damage,				
power cables should be segregated from communications cables to prevent interference;				
clearly identifiable cable and equipment markings should be used to minimise handling errors, such as accidental patching of wrong network cables;				
a documented patch list should be used to reduce the possibility of errors;				
for sensitive or critical systems further controls to consider include: 1) installation of armoured conduit and locked rooms or boxes at inspection and termination points; 2) use of alternative routings and/or transmission media providing appropriate security; 3) use of fibre optic cabling; 4) use of electromagnetic shielding to protect the cables; 5) initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables; 6) controlled access to patch panels and cable rooms;				

9.2.4 Equipment maintenance management

Control

Equipment should be correctly maintained to ensure its continued availability and integrity.

Question	Yes	Partially	No	Comments
equipment should be maintained in accordance with the supplier's recommended service intervals and specifications;				
only authorized maintenance personnel should carry out repairs and service equipment;				
records should be kept of all suspected or actual faults, and all preventive and corrective maintenance;				
appropriate controls should be implemented when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organization;				
all requirements imposed by insurance policies should be complied with.				

9.2.5 Security of equipment off-premises

Control

Security should be applied to off-site equipment taking into account the different risks of working outside the organization's premises.

Question	Yes	Partially	No	Comments
Regardless of ownership, the use of any information processing equipment outside the organization's premises should be authorized by management.				
equipment and media taken off the premises should not be left unattended in public places;				
manufacturers' instructions for protecting equipment should be observed at all times,				
home-working controls should be determined by a risk assessment and suitable controls applied as				

appropriate, e.g. lockable filing cabinets, clear desk policy, access controls for computers and secure communication with the office				
adequate insurance cover should be in place to protect equipment off-site.				

9.2.6 Secure disposal or re-use of equipment management

Control
All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

Question	Yes	Partially	No	Comments
Devices containing sensitive information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.				

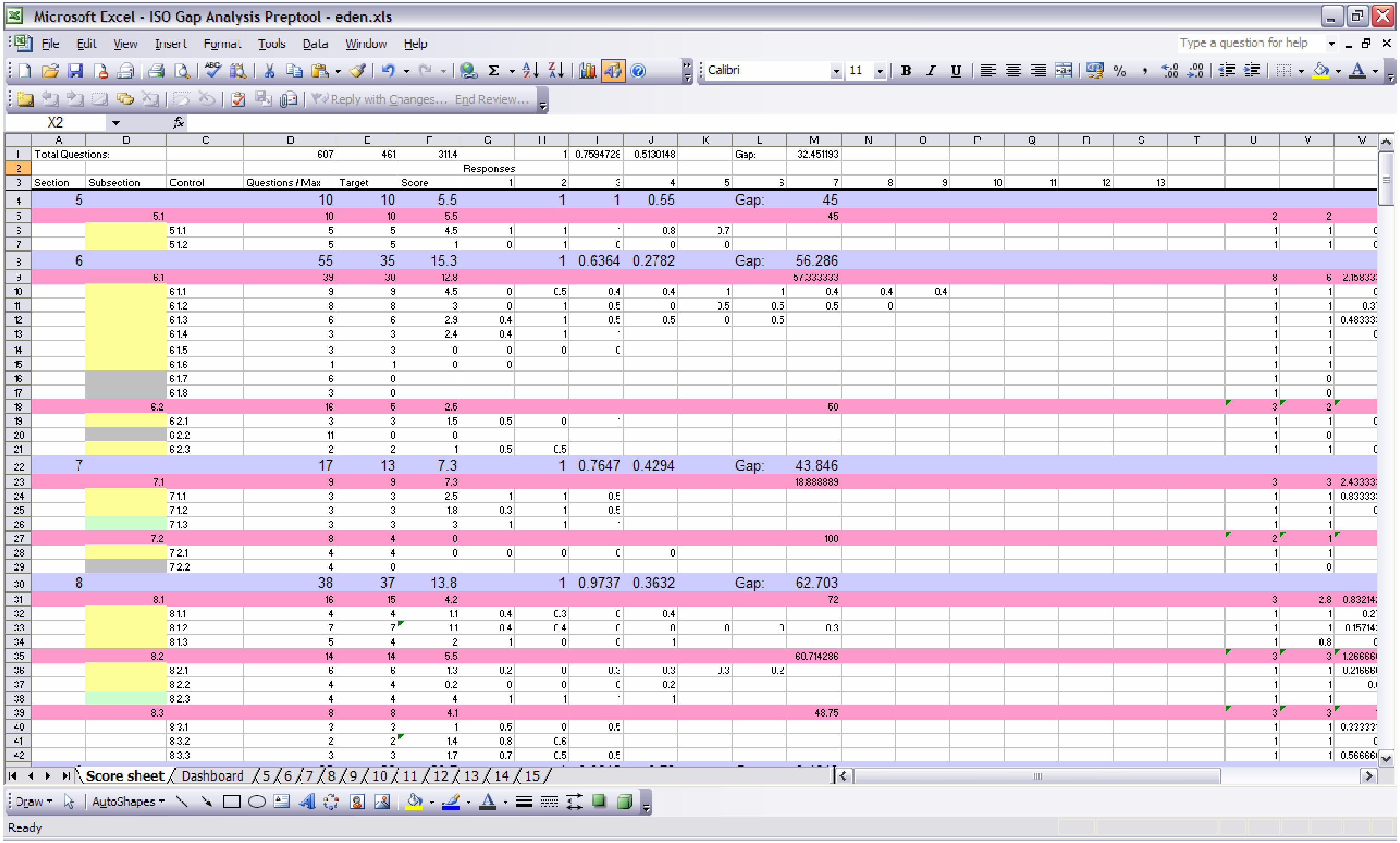
9.2.7 Removal of property documents

Control
Equipment, information or software should not be taken off-site without prior authorization.

Question	Yes	Partially	No	Comments
equipment, information or software should not be taken off-site without prior authorization;				
employees, contractors and third party users who have authority to permit off-site removal of assets should be clearly identified;				
time limits for equipment removal should be set and returns checked for compliance;				
where necessary and appropriate, equipment should be recorded as being removed off-site and recorded when returned.				

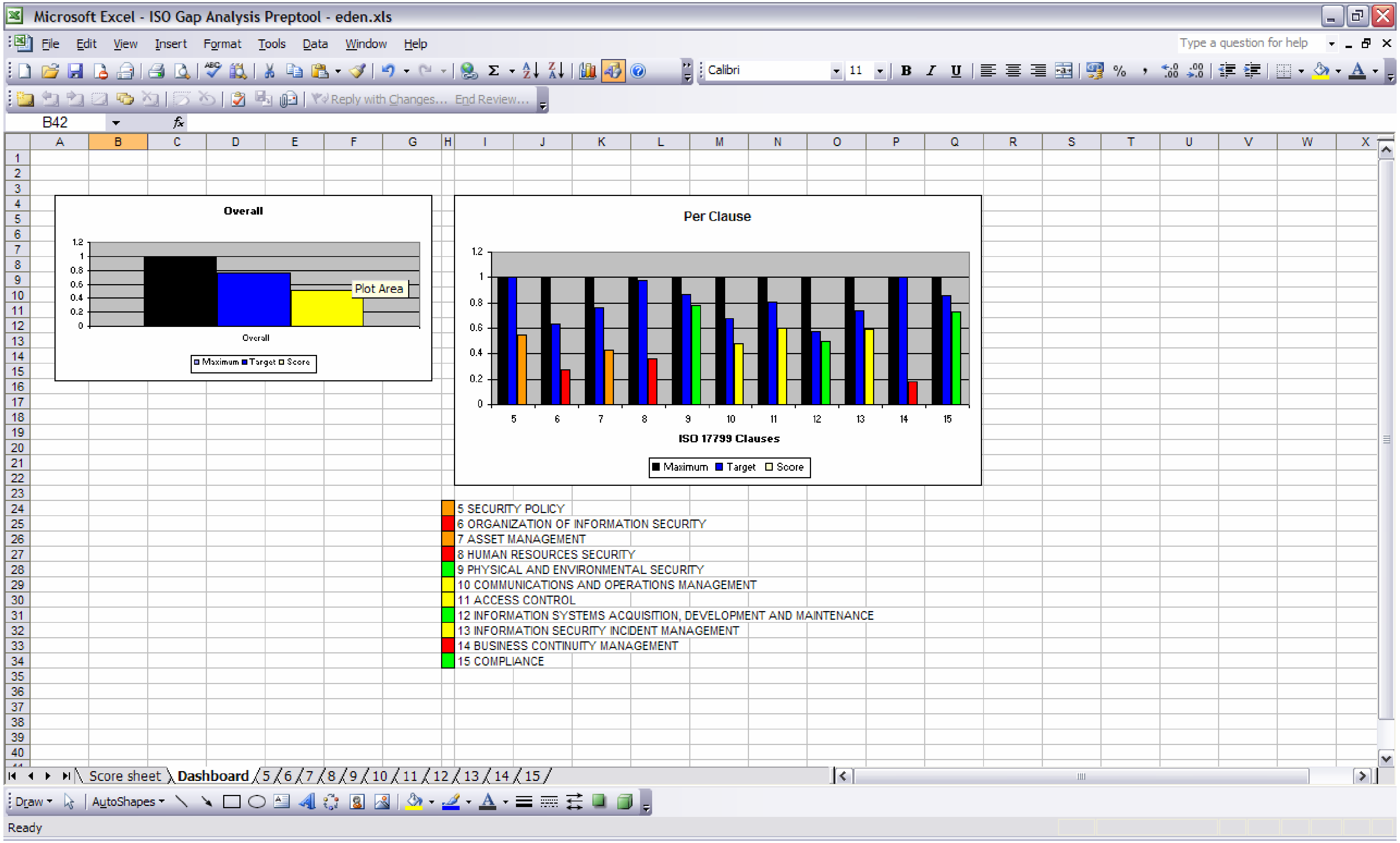
Appendix D

The ISO 17799 Analysis Tool

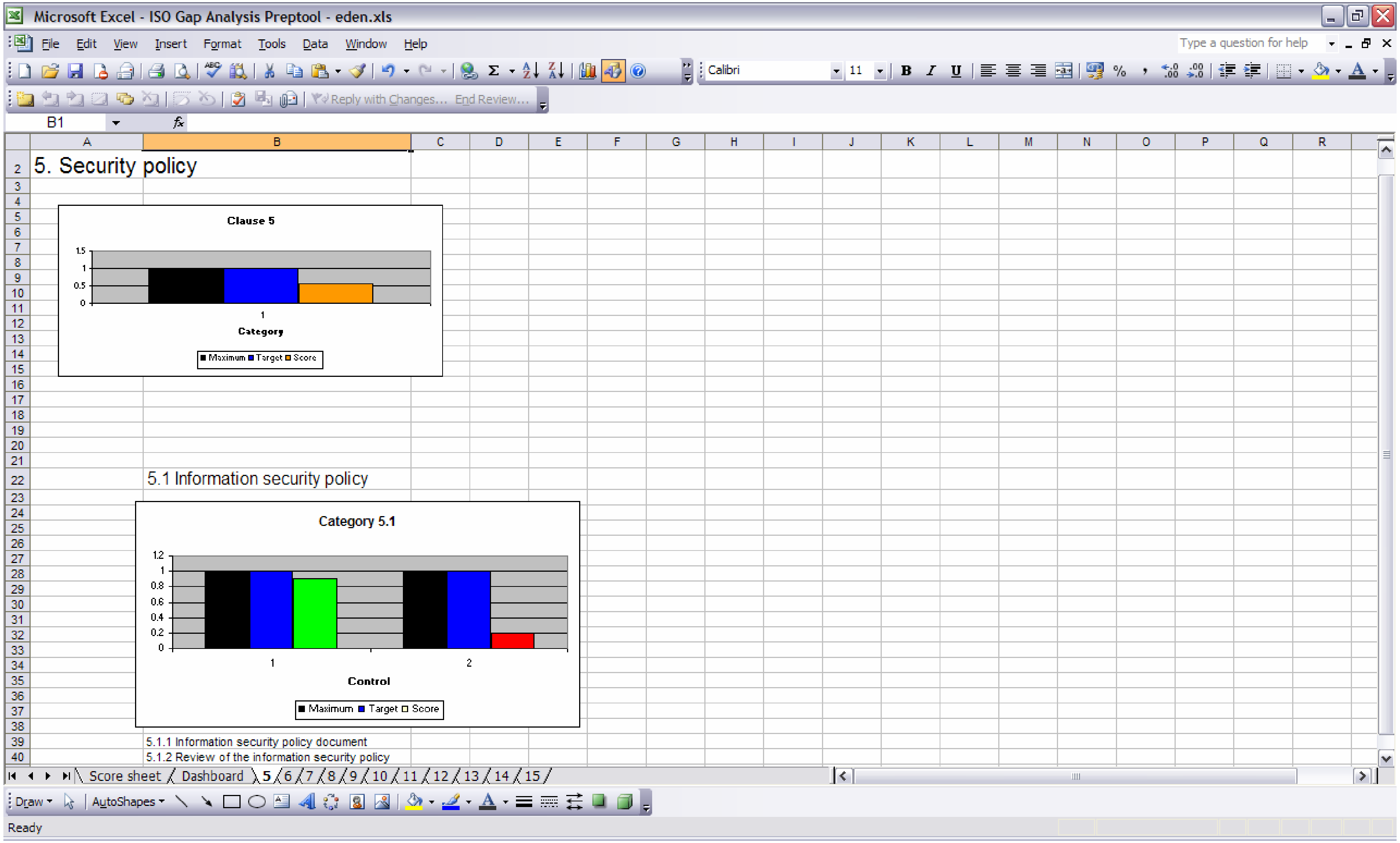


Microsoft Excel - ISO Gap Analysis Preptool - eden.xls

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
1	Total Questions:			607	461	311.4		1	0.7594728	0.5130148		Gap:	32.451193										
2							Responses																
3	Section	Subsection	Control	Questions / Max	Target	Score	1	2	3	4	5	6	7	8	9	10	11	12	13				
4	5			10	10	5.5		1	1	0.55		Gap:	45										
5		5.1		10	10	5.5							45								2	2	
6			5.1.1	5	5	4.5	1	1	1	0.8	0.7										1	1	0
7			5.1.2	5	5	1	0	1	0	0	0										1	1	0
8	6			55	35	15.3		1	0.6364	0.2782		Gap:	56.286										
9		6.1		39	30	12.8							57.333333								8	6	2.15833
10			6.1.1	9	9	4.5	0	0.5	0.4	0.4	1	1	0.4	0.4	0.4						1	1	0
11			6.1.2	8	8	3	0	1	0.5	0	0.5	0.5	0.5	0							1	1	0.3
12			6.1.3	6	6	2.9	0.4	1	0.5	0.5	0	0.5									1	1	0.48333
13			6.1.4	3	3	2.4	0.4	1	1												1	1	0
14			6.1.5	3	3	0	0	0	0												1	1	
15			6.1.6	1	1	0	0														1	1	
16			6.1.7	6	0																1	0	
17			6.1.8	3	0																1	0	
18		6.2		16	5	2.5							50								3	2	
19			6.2.1	3	3	1.5	0.5	0	1												1	1	0
20			6.2.2	11	0	0															1	0	
21			6.2.3	2	2	1	0.5	0.5													1	1	0
22	7			17	13	7.3		1	0.7647	0.4294		Gap:	43.846										
23		7.1		9	9	7.3							18.888889								3	3	2.43333
24			7.1.1	3	3	2.5	1	1	0.5												1	1	0.83333
25			7.1.2	3	3	1.8	0.3	1	0.5												1	1	0
26			7.1.3	3	3	3	1	1	1												1	1	
27		7.2		8	4	0							100								2	1	
28			7.2.1	4	4	0	0	0	0	0											1	1	
29			7.2.2	4	0																1	0	
30	8			38	37	13.8		1	0.9737	0.3632		Gap:	62.703										
31		8.1		16	15	4.2							72								3	2.8	0.83214
32			8.1.1	4	4	1.1	0.4	0.3	0	0.4											1	1	0.2
33			8.1.2	7	7	1.1	0.4	0.4	0	0	0	0	0.3								1	1	0.15714
34			8.1.3	5	4	2	1	0	0	1											1	0.8	0
35		8.2		14	14	5.5							60.714286								3	3	1.26666
36			8.2.1	6	6	1.3	0.2	0	0.3	0.3	0.3	0.2									1	1	0.21666
37			8.2.2	4	4	0.2	0	0	0	0.2											1	1	0.
38			8.2.3	4	4	4	1	1	1	1											1	1	
39		8.3		8	8	4.1							48.75								3	3	
40			8.3.1	3	3	1	0.5	0	0.5												1	1	0.33333
41			8.3.2	2	2	1.4	0.8	0.6													1	1	0
42			8.3.3	3	3	1.7	0.7	0.5	0.5												1	1	0.56666



🟧 5 SECURITY POLICY
🟥 6 ORGANIZATION OF INFORMATION SECURITY
🟧 7 ASSET MANAGEMENT
🟥 8 HUMAN RESOURCES SECURITY
🟩 9 PHYSICAL AND ENVIRONMENTAL SECURITY
🟨 10 COMMUNICATIONS AND OPERATIONS MANAGEMENT
🟨 11 ACCESS CONTROL
🟩 12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE
🟨 13 INFORMATION SECURITY INCIDENT MANAGEMENT
🟥 14 BUSINESS CONTINUITY MANAGEMENT
🟩 15 COMPLIANCE

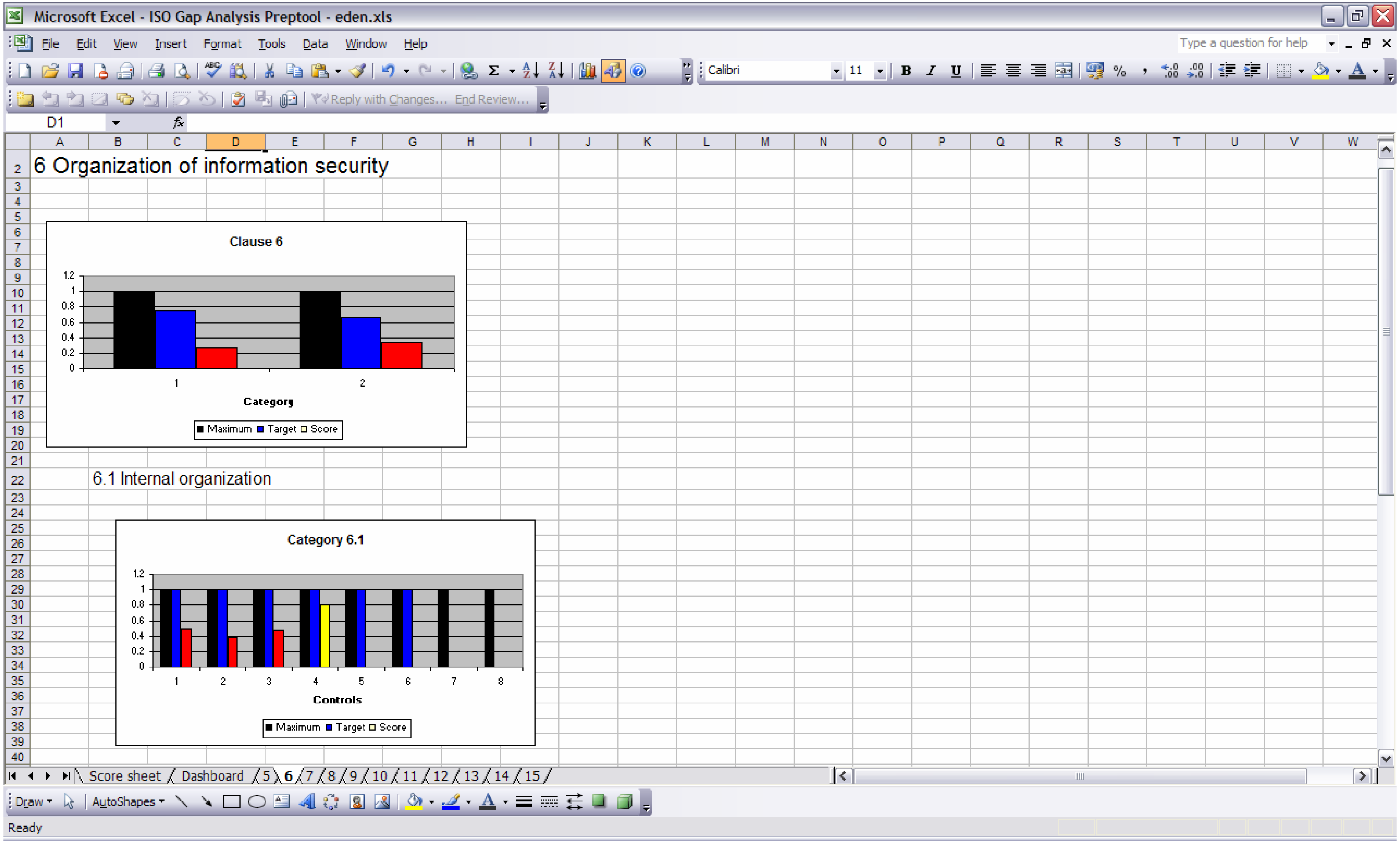


5. Security policy

5.1 Information security policy

5.1.1 Information security policy document

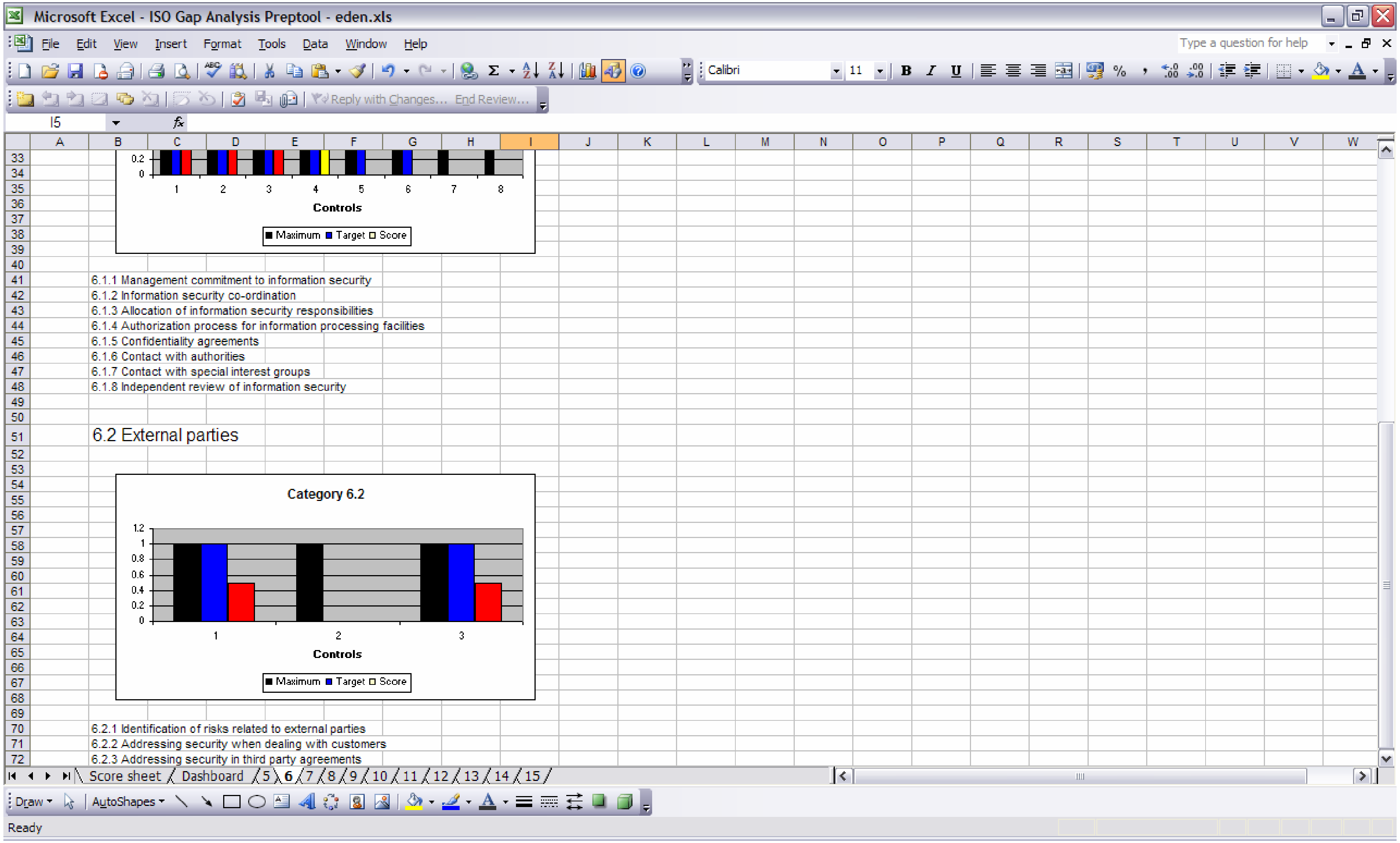
5.1.2 Review of the information security policy



Microsoft Excel - ISO Gap Analysis Preptool - eden.xls

6 Organization of information security

6.1 Internal organization



6.1.1 Management commitment to information security
6.1.2 Information security co-ordination
6.1.3 Allocation of information security responsibilities
6.1.4 Authorization process for information processing facilities
6.1.5 Confidentiality agreements
6.1.6 Contact with authorities
6.1.7 Contact with special interest groups
6.1.8 Independent review of information security

6.2 External parties

6.2.1 Identification of risks related to external parties
6.2.2 Addressing security when dealing with customers
6.2.3 Addressing security in third party agreements

This appendix contains the screenshots from the tool that is representative of the various levels within ISO 17799, Dashboard and 2 security categories, categories 5 and 6. The other 9 security categories have the same look and functionality as the above screenshots. Category 5 and 6 provide sufficient information and no new information would be gained if the other 9 categories' screens were also added.

Appendix E

Executive Summary of the IT Strategic Objective Plan (IT-SOP)

Introduction (Executive Summary)

This document, the IT-SOP is part of the Information Technology Governance framework. It is discussed in the accompanying IT Governance report.

The ultimate objective of Eden DM is to implement the supplied control objectives at the following maturity levels:

Domain / Number	1	2	3	4	5	6	7	8	9	10	11	12	13
PO	4	4	4	4	4	4	4	4	4	4	4		
AI	4	4	4	4	4	4							
DS	4	4	4	4	5	3	4	4	4	4	5	4	4
M	4	4	4	4									

In order to achieve this objective, the control objectives have been grouped in phases. These phases are designed to implement the most important processes first, accounting for most of the current problem situations. In order to ease implementation and the management thereof, the objectives have been limited to between 4 and 6 objectives per phase:

These phases are as follows:

IT-SOP Phase 1: PO1, PO4, AI6, DS4, DS5
IT-SOP Phase 2: PO6, PO7, PO9, DS1, DS2
IT-SOP Phase 3: PO8, DS7, DS10, DS11, DS12
IT-SOP Phase 4: The remainder of the objectives.

After the first 3 phases are complete, it is up to Eden DM to define additional strategic phases containing the rest of the objectives to be implemented in order to ultimately implement all 34 CobiT objectives.

Appendix F

The IT Strategic Objective Plan (IT-SOP)

PO 1 – Define a strategic IT plan

Strike balance between technology opportunities and IT business requirements

For the PO1 objective to be implemented successfully in the municipality, it needs to implement the detailed control objectives, as well as the corresponding ISO 17799 security controls, at a managed and measurable level by measuring its compliance against the critical success factors (CSF) and measuring performance against the key performance indicators (KPI).

In order to meet the Managed and Measurable governance level, the following steps are necessary:

1. Create awareness throughout the municipality that strategic IT planning is needed.

2. Identify and define procedures in order to perform strategic IT planning in the municipality.

3. Document these procedures and assign the responsibility to perform them to the designated authority.

4. Manage and Monitor the process of strategic IT planning with the use of the CSF and KPI.

Desired Maturity Model

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. With respect to the IT strategic planning process, management is able to monitor it, 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 organisation-wide strategy are increasingly becoming more coordinated by addressing business processes and value-added capabilities and by leveraging the use of applications and technologies through business process re-engineering. There is a well-defined process for balancing the internal and external resources required in system development and operations. Benchmarking against industry norms and competitors is becoming increasingly formalised.

High-level Security Requirements

No High-level 17799 section is mapped directly to PO1.

Control Objectives

As per COBIT Mapping between COBIT version 3 and ISO 17799: 2000 document

PO1.1 IT as Part of the Organization's Long- and Short-range Plan

Senior management is responsible for developing and implementing long- and short-range plans that fulfill the organization's mission and goals. In this respect, senior management should ensure that IT issues and opportunities are adequately assessed and reflected in the organization's long- and short-range plans. IT long- and short-range plans should be developed to help ensure that the use of IT is aligned with the mission and business strategies of the organization.

17799 requirement(s):

- Security has to be part of the strategic planning (4.1.2).

PO1.2 IT Long-range Plan

IT management and business process owners are responsible for regularly developing IT long-range plans supporting the achievement of the organization's overall missions and goals. The planning approach should include mechanisms to solicit input from relevant internal and external stakeholders impacted by the IT strategic plans. Accordingly, management should implement a long-range planning process, adopt a structured approach and set up a standard plan structure.

17799 requirement(s):

- The management information security forum shall approve the security-relevant initiatives (4.1.1).

PO1.3 IT Long-range Planning—Approach and Structure

IT management and business process owners should establish and apply a structured approach regarding the long-range planning process. This should result in a high-quality plan which covers the basic questions of what, who, how, when and why. The IT planning process should take into account risk assessment results, including business, environmental, technology and human resources risks. Aspects that need to be taken into account and adequately addressed during the planning process include the organizational model and changes to it, geographical distribution, technological evolution, costs, legal and regulatory requirements, requirements of third parties or the market, planning horizon, business process reengineering, staffing, in- or outsourcing, data, application systems and technology architectures. Benefits of the choices made should be clearly identified. The IT long- and short-range plans should incorporate performance indicators and targets. The plan itself should also refer to other plans, such as the organization quality plan and the information risk management plan.

17799 requirement(s):

- Not addressed in ISO/IEC17799

PO1.4 IT Long-range Plan Changes

IT management and business process owners should ensure that a process is in place to modify the IT long-range plan in a timely and accurate manner to accommodate changes to the organization's long-range plan and changes in IT conditions. Management should establish a policy requiring that IT long- and short-range plans are developed and maintained.

17799 requirement(s):

- Not addressed in ISO/IEC17799

PO1.5 Short-range Planning for the IT Function

IT management and business process owners should ensure that the IT long-range plan is regularly translated into IT short-range plans. Such short-range plans should ensure that appropriate IT function resources are allocated on a basis consistent with the IT long-range plan. The short-range plans should be reassessed periodically and amended as necessary in response to changing business and IT conditions. The timely performance of feasibility studies should ensure that the execution of the short-range plans is adequately initiated.

17799 requirement(s):

- The management information security forum shall approve the security relevant initiatives (4.1.1).

PO1.6 Communication of IT Plans

Management should ensure that IT long- and short-range plans are communicated to business process owners and other relevant parties across the organization.

17799 requirement(s):

- The information security forum should show support of the information security (4.1.2).

PO1.7 Monitoring and Evaluating of IT Plans

Management should establish processes to capture and report feedback from business process owners and users regarding the quality and usefulness of long- and short-range plans. The feedback obtained should be evaluated and considered in future IT planning.

17799 requirement(s):

- Not addressed in ISO/IEC17799

PO1.8 Assessment of Existing Systems

Prior to developing or changing the strategic or long-range IT plan, IT management should assess the existing information systems in terms of degree of business automation, functionality, stability, complexity, costs, strengths and weaknesses to determine the degree to which the existing systems support the organization's business requirements.

17799 requirement(s):

- Information security management is responsible for monitoring information assets, especially in the case of significant changes (4.1.1).

Critical Success Factors

- The planning process provides for a prioritisation scheme for the business objectives and quantifies, where possible, the business requirements
- Management buy-in and support is enabled by a documented methodology for the IT strategy development, the support of validated data and a structured, transparent decision-making process
- The IT strategic plan clearly states a risk position, such as leading edge or road-tested, innovator or follower, and the required balance between time-to-market, cost of ownership and service quality
- All assumptions of the strategic plan have been challenged and tested
- The processes, services and functions needed for the outcome are defined, but are flexible and changeable, with a transparent change control process
- A reality check of the strategy by a third party has been conducted to increase objectivity and is repeated at appropriate times
- IT strategic planning is translated into roadmaps and migration strategies

Key Performance Indicators

- Age of IT strategic plan (number of months since last update)
- Percent of participant satisfaction with the IT strategic planning process
- Time lag between change in the IT strategic plans and changes to operating plans
- Index of participants involved in strategic IT plan development, based on size of effort, ratio of involvement of business owners to IT staff and number of key participants
- Index of quality of the plan, including timelines of development effort, adherence to structured approach and completeness of plan

PO 4 – Define the IT organisation and relationships

To deliver the right IT services

For the PO4 objective to be implemented successfully in the municipality, it needs to implement the detailed control objectives, as well as the corresponding ISO 17799 security controls, at a managed and measurable level by measuring its compliance against the critical success factors (CSF) and measuring performance against the key performance indicators (KPI).

In order to meet the Managed and Measurable governance level, the following steps are necessary:

1. Create awareness throughout the municipality that it is required to define its IT organisation and its relationships.

2. Identify and define procedures in order to define the IT organisation and its relationships of the municipality.

3. Document these procedures and assign the responsibility to perform them to the designated authority.

4. Manage and Monitor the process of defining the IT organisation and its relationships with the use of the CSF and KPI.

Desired Maturity Model

Managed and Measurable

The IT organisation is sophisticated, proactively responds to change and includes all roles necessary to meet business requirements. IT management, process ownership, accountability and responsibility are defined and balanced. Essential IT staffing requirements and expertise needs are satisfied. Internal best practices have been applied in the organisation of the IT functions. IT management has the appropriate expertise and skills to define, implement and monitor the preferred organisation and relationships. Measurable metrics to support business objectives and user defined critical success factors are standardised. Skill inventories are available to support project staffing and professional development. The balance between the skills and resources available internally and those needed from external organisations is defined and enforced.

High-level Security Requirements

The following high-level 17799 mappings were made to PO4:

- 4.1 Information Security Infrastructure
- 5.1 Accountability for assets
- 6.1 Security in Job definition and resourcing
- 8.1 Operational procedures and responsibilities

Control Objectives

As per COBIT Mapping between COBIT version 3 and ISO 17799: 2000 document

PO4.1 IT Planning or Steering Committee

The organization's senior management should appoint a planning or steering committee to oversee the IT function and its activities. Committee membership should include representatives from senior management, user management and the IT function. The committee should meet regularly and report to senior management.

17799 requirement(s):

- There should be a management forum, which is responsible for promoting security and for approving major activities (4.1.1).

PO4.2 Organizational Placement of the IT Function

In placing the IT function in the overall organization structure, senior management should ensure authority, critical mass and independence from user departments to the degree necessary to guarantee effective IT solutions and sufficient progress in implementing them, and to establish a partnership relation with top management to help increase awareness, understanding, and skill in identifying and resolving IT issues.

17799 requirement(s):

- The information security organization should draw on specialist advice to ensure expertise and skill.
- In addition, a multidisciplinary and cross-functional approach to implementing the information security function enables partnership, business support and effective security solutions.
- Access to management throughout the organization enables the requisite independence for maximum effectiveness (4.1.1 to 4.1.5).

PO4.3 Review of Organizational Achievements

A framework should be in place for reviewing the organizational structure to continuously meet objectives and changing circumstances.

17799 requirement(s):

- The management information security forum should review and approve the information security policy and the overall responsibilities (4.1.1).

PO4.4 Roles and Responsibilities

Management should ensure that all personnel in the organization have and know their roles and responsibilities in relation to information systems. All personnel should have sufficient authority to exercise the role and responsibility assigned to them. Roles should be designed with consideration to appropriate segregation of duties. No one individual should control all key aspects of a transaction or event. Everyone should be made aware that they have some degree of responsibility for internal control and security. Consequently, regular campaigns should be organized and undertaken to increase awareness and discipline.

17799 requirement(s):

- Responsibility for protection should be defined for individual assets (4.1.3).
- The job descriptions should include responsibility for security (6.1.1).
- All responsibilities and procedures for the management and operation of information systems should be defined and implemented, including segregation of duties, incident response and security controls.
- Awareness and training should be provided to ensure the establishment of security roles and responsibilities (6.2, 8.1.1, 8.1.2, 8.1.3, 8.1.4).
- A data protection officer should be nominated (12.1.4).

PO4.5 Responsibility for Quality Assurance

Management should assign the responsibility for the performance of the quality assurance function to staff members of the IT function and ensure that appropriate quality assurance, systems, controls and communications expertise exist in the IT function's quality assurance group. The organizational placement within the IT function and the responsibilities and the size of the quality assurance group should satisfy the requirements of the organization.

17799 requirement(s):

- Not addressed in ISO/IEC17799

PO4.6 Responsibility for Logical and Physical Security

Management should formally assign the responsibility for assuring the logical and physical security of the organization's information assets to an information security manager, reporting to the organization's senior management. At a minimum, security management responsibility should be established at the organization-wide level to deal with overall security issues in an organization. If needed, additional security management responsibilities should be assigned at a system-specific level to cope with the related security issues.

17799 requirement(s):

- It is the responsibility of a suitable management information security forum to define direction for and support of information security. The activities typically performed by this forum should be provided (4.1.1).
- Representatives from different parts of the organization that form the management forum should initiate and oversee implementation of information security controls. The activities of that cross functional forum are listed (4.1.2).
- Responsibility for protection should be defined for individual assets (4.1.3).
- The identification, definition and implementation of relevant controls should be the responsibility of an information security officer, as appropriate (4.1.3).
- Where security-relevant expertise is not available in-house, external expertise should be gathered, and an in-house security adviser should manage the coordination of in-house and external sources for information and advice (4.1.5).
- The management of information security and responsibility for security should follow an overall framework (4.1.6).
- Responsibility of security should be managed throughout the engagement of staff and third-party users. All individuals who have access to confidential or secret information processing facilities should sign a nondisclosure agreement (6.1).
- Definition and documentation of the roles and responsibilities should be as specific as appropriate. The responsibility for implementation and maintenance of the security policy and specific processes or activities should be included (6.1.1).
- A data protection officer should be nominated (12.1.4).

PO4.7 Ownership and Custodianship

Management should create a structure for formally appointing the data owners and custodians. Their roles and responsibilities should be clearly defined.

17799 requirement(s):

- The information security policy should contain the requirement of and guidance for the definition of security roles and responsibilities (4.1.3).
- A dedicated owner for major information assets should be nominated (5.1).

PO4.8 Data and System Ownership

Management should ensure that all information assets (data and systems) have an appointed owner who makes decisions about classification and access rights. System owners typically delegate day-today custodianship to the systems delivery/operations group and delegate security responsibilities to a security administrator. Owners, however, should remain accountable for the maintenance of appropriate security measures.

17799 requirement(s):

- Ownership of and responsibility for information assets should be defined. Whereas day-to-day activities may be delegated to individuals, ultimate responsibility should remain with the owner of the information asset (4.1.3).
- A dedicated owner for major information assets should be nominated. The owner should be responsible for maintenance of appropriate protection (5.1).

PO4.9 Supervision

Senior management should implement adequate supervisory practices in the IT function to ensure that roles and responsibilities are properly exercised, to assess whether all personnel have sufficient authority and resources to execute their roles and responsibilities, and to generally review key performance indicators.

17799 requirement(s):

- A management information security forum should assess the adequacy of security controls and coordinate their implementation (4.1.2).
- Although the responsibility for implementation of the security controls for information assets may be delegated to individuals, the responsibility should remain with the owner (4.1.3).
- Accountability should remain with the owner of the information asset. The owner must supervise delegated activities or assess that the responsibility has been discharged appropriately (5.1).

PO4.10 Segregation of Duties

Senior management should implement a division of roles and responsibilities, which should exclude the possibility for a single individual to subvert a critical process. Management should also make sure that personnel are performing only those duties stipulated for their respective jobs and positions. In particular, a segregation of duties should be maintained among the following functions:

– Information systems use

– Data entry

– Computer operation

– Network management

– System administration

– Systems development and maintenance

– Change management

– Security administration

– Security audit

17799 requirement(s):

- The demand for segregation of duties should be stated and a list of requirements for this segregation provided. In addition, the need for segregated environments to enable the implementation of the necessary segregated roles should be stated (8.1.4, 8.1.5).
- Computer operation should be segregated from operational responsibility (8.5.1).
- Separation of duties should be considered for log reviews (9.7.2).

PO4.11 IT Staffing

Staffing requirements evaluations should be performed regularly to ensure that the IT function has a sufficient number of competent IT staff. Staffing requirements should be evaluated at least annually or upon major changes to the business, operational or IT environment. Evaluation results should be acted upon promptly to ensure adequate staffing now and in the future.

17799 requirement(s):

- Not addressed in ISO/IEC17799

PO4.12 Job or Position Descriptions for IT Staff

Management should ensure that position descriptions for IT staff are established and updated regularly. These position descriptions should clearly delineate both authority and responsibility, include definitions of skills and experience needed in the relevant position, and be suitable for use in performance evaluation.

17799 requirement(s):

- Definition and documentation of the roles and responsibilities should be as specific as appropriate. The responsibility for implementation and maintenance of the security policy and specific processes or activities should be included (6.1.1).

PO4.13 Key IT Personnel

IT management should define and identify key IT personnel.

17799 requirement(s):

- Not addressed in ISO/IEC17799

PO4.14 Contracted Staff Policies and Procedures

Management should define and implement relevant policies and procedures for controlling the activities of consultants and other contract personnel by the IT function to assure the protection of the organization’s information assets.

17799 requirement(s):

- Information for suitable policies and procedures should include the security requirements and internal controls to administer access to information and monitor the activities of onsite contractors (4.2.1.3).
- Detailed requirements for contracts with third parties should address the security-relevant issues that are listed in the ISO standard (4.2.2).
- Confidentiality agreements should be required from third parties and temporary staff (6.1.3).
- Access of third parties to secure areas should be monitored (7.1.4).
- Computer misuse should be documented and logged (12.1.5).

PO4.15 Relationships

IT management should undertake the necessary actions to establish and maintain an optimal coordination, communication and liaison structure between the IT function and various other interests inside and outside the IT function (i.e., users, suppliers, security officers, risk managers).

17799 requirement(s):

- Establishing appropriate contacts with external parties, such as relevant law enforcement authorities, regulatory bodies, telecom providers, membership of industry forum and security groups, should be considered. In addition, the management for information security should consider cooperation with internal parties, such as managers, users, administrators, designers, auditors and other security staff (4.1).

Critical Success Factors

- The IT organisation communicates its goals and results at all levels
- IT is organised to be involved in all decision processes, respond to key business initiatives and focus on all corporate automation needs
- The IT organisational model is aligned with the business functions and adapts rapidly to changes in the business environment
- Through encouraging and promoting the taking of responsibility, an IT organisation develops and grows individuals and heightens collaboration
- There are clear command and control processes, with segregation where needed, specialisation where required and empowerment where beneficial
- The IT organisation properly positions security, internal control and quality functions, and adequately balances supervision and empowerment
- The IT organisation is flexible to adapt to risk and crisis situations and moves from a hierarchical model, when all is well, to a team-based model when pressure mounts, empowering individuals in times of crisis
- Strong management control is established over the outsourcing of IT services, with a clear policy, and awareness of the total cost of outsourcing
- Essential IT functions are explicitly identified in the organisation model, with clearly specified roles and responsibilities

Key Performance Indicators

- Age of organisational change, including reorganisation or organisational reassessment
- Number of organisational assessment recommendations not acted upon
- Percent of IT organisational functions which are mapped into the business organisational structure
- Number of IT units with business objectives directly cascaded into individual roles and responsibilities
- Percent of roles with documented position descriptions
- Average lag time between change in business direction and the reflection of the change in the IT organisational structure
- Percent of essential functions which are explicitly identified in the organisational model with clear roles and responsibilities

AI 6 – Manage Changes

Minimizing the likelihood of disruption, unauthorized alterations and errors.

For the AI6 objective to be implemented successfully in the municipality, it needs to implement the detailed control objectives, as well as the corresponding ISO 17799 security controls, at a managed and measurable level by measuring its compliance against the critical success factors (CSF) and measuring performance against the key performance indicators (KPI).

In order to meet the Managed and Measurable governance level, the following steps are necessary:

1. Create awareness throughout the municipality that it is required to manage changes.

2. Identify and define procedures in order to manage changes of the municipality.

3. Document these procedures and assign the responsibility to perform them to the designated authority.

4. Manage and Monitor the process of change management with the use of the CSF and KPI.

Desired Maturity Model

Managed and Measurable

The change management process is well developed and consistently followed for all changes and management is confident that there are no exceptions. The process is efficient and effective, but relies on considerable manual procedures and controls to ensure that quality is achieved. All changes are subject to thorough planning and impact assessment to minimise the likelihood of post-production problems. An approval process for changes is in place. Change management documentation is current and correct, with changes formally tracked. Configuration documentation is generally accurate. IT change management planning and implementation is becoming more integrated with changes in the business processes, to ensure that training, organisational changes and business continuity issues are addressed. There is increased co-ordination between IT change management and business process re-design.

High-level Security Requirements

The following high-level 17799 mappings were made to AI6:

- 10.5 Security in development and support processes

Control Objectives

As per COBIT Mapping between COBIT version 3 and ISO 17799: 2000 document

AI6.1 Change Request Initiation and Control

IT management should ensure that all requests for changes, system maintenance and supplier maintenance should be standardized and subject to formal change management procedures. Changes should be categorized and prioritized and specific procedures should be in place to handle urgent matters. Change requesters should be kept informed about the status of their request.

17799 requirement(s):

- The manager responsible for maintenance should approve compliance with security policies and requirements (4.1.4).
- Requirements for compliance with the organization's change management process should be included in third-party contracts (4.2.2).
- Software malfunctions should be reported according to defined procedures. If required, the services should be stopped. Messages should be noted to facilitate investigation of problems, and security managers should be informed. Only trained and experienced staff should be responsible for error corrections (6.3.3).
- To prevent system or security failures, changes to systems should be performed in a strictly controlled manner. Audit logs should contain relevant information on the changes. Impacts on operational systems should be considered. Detailed controls are recommended in the ISO standard (8.1.2).
- There should be no changes to the project or support environment without appropriate security reviews (10.5).
- Changes should follow strict change control procedures. Operational and application change control processes should be integrated. Detailed requirements are listed in the ISO standard (10.5.1).
- Software packages should be modified only if required. Modifications to software packages should consider vendor approval and ensure future maintainability (10.5.3).

AI6.2 Impact Assessment

A procedure should be in place to ensure that all requests for change are assessed in a structured way for all possible impacts on the operational system and its functionality.

17799 requirement(s):

- Potential impacts of changes should be part of the change control process (8.1.2).
- Future maintenance as well as other risks (impact on integrated controls, consent of vendor, etc.) should be considered when software packages are modified (10.5.3).

AI6.3 Control of Changes

IT management should ensure that change management and software control and distribution are properly integrated with a comprehensive configuration management system. The system used to monitor changes to application systems should be automated to support the recording and tracking of changes made to large, complex information systems.

17799 requirement(s):

- Changes to operating systems should be reviewed accordingly (6.3).
- Maintenance activities (preventive and corrective) and faults should be recorded (7.2.4).
- Technical reviews should be performed in case of operating system changes (10.5.2).

AI6.4 Emergency Changes

IT management should establish parameters defining emergency changes and procedures to control these changes when they circumvent the normal process of technical, operational and management assessment prior to implementation. The emergency changes should be recorded and authorized by IT management prior to implementation.

17799 requirement(s):

- Emergency actions should be documented in detail (8.1.3).
- Emergency changes should follow defined procedures (10.5.1).

AI6.5 Documentation and Procedures

The change process should ensure that, whenever system changes are implemented, the associated documentation and procedures are updated accordingly.

17799 requirement(s):

- Maintenance of controls, documentation and procedures should be the responsibility of the information asset's nominated owner (5.1).
- Changes to operating systems should consider an update of business continuity plans (6.3, 11.1.5.2).
- Change management procedures should require updating the relevant documentation (10.5.1).
- Technical reviews should be performed in case of operating system changes (10.5.2).

AI6.6 Authorized Maintenance

IT management should ensure that maintenance personnel have specific assignments and that their work is properly monitored. In addition, their system access rights should be controlled to avoid risks of unauthorized access to automated systems.

17799 requirement(s):

- Maintenance should be defined in outsourcing contracts (4.1.3).
- Third-party access should be authorized, monitored and controlled (4.2).
- The responsible manager should approve compliance with relevant security policies and requirements (4.1.4).
- Physical separation of equipment managed by third parties should be considered (7.1.3).
- Only authorized personnel should perform repairs and services (7.2.4).

AI6.7 Software Release Policy

IT management should ensure that the release of software is governed by formal procedures ensuring sign-off, packaging, regression testing, handover, etc.

17799 requirement(s):

- Releases should be controlled and formal approval should be obtained before rollout. Changes should minimize negative impacts on business processes. Detailed controls are provided in the ISO standard (10.5.1).

AI6.8 Distribution of Software

Specific internal control measures should be established to ensure distribution of the correct software element to the right place, with integrity, in a timely manner and with adequate audit trails.

17799 requirement(s):

- Releases should be controlled and formal approval should be obtained before rollout. Changes should minimize negative impacts on business processes. Detailed controls are provided in the ISO standard (10.5.1).

Critical Success Factors

- Change policies are clear and known and they are rigorously and systematically implemented
- Change management is strongly integrated with release management and is an integral part of configuration management
- There is a rapid and efficient planning, approval and initiation process covering identification, categorisation, impact assessment and prioritisation of changes
- Automated process tools are available to support workflow definition, pro-forma work plans, approval templates, testing, configuration and distribution
- Expedient and comprehensive acceptance test procedures are applied prior to making the change
- A system for tracking and following individual changes, as well as change process parameters, is in place
- A formal process for hand-over from development to operations is defined
- Changes take the impact on capacity and performance requirements into account
- Complete and up-to-date application and configuration documentation is available
- A process is in place to manage co-ordination between changes, recognising interdependencies
- An independent process for verification of the success or failure of change is implemented
- There is segregation of duties between development and production

Key Performance Indicators

- Number of different versions installed at the same time
- Number of software release and distribution methods per platform
- Number of deviations from the standard configuration
- Number of emergency fixes for which the normal change management process was not applied retroactively
- Time lag between the availability of the fix and its implementation
- Ratio of accepted to refused change implementation requests

DS 4 – Ensure Continuous Service

IT services are available as required and to ensure a minimum business impact in the event of a major disruption

For the DS4 objective to be implemented successfully in the municipality, it needs to implement the detailed control objectives, as well as the corresponding ISO 17799 security controls, at a managed and measurable level by measuring its compliance against the critical success factors (CSF) and measuring performance against the key performance indicators (KPI).

In order to meet the Managed and Measurable governance level, the following steps are necessary:

1. Create awareness throughout the municipality that it is required to ensure continuity of the IT function.

2. Identify and define procedures in order to ensure continuous IT services of the municipality.

3. Document these procedures and assign the responsibility to perform them to the designated authority.

4. Manage and Monitor the process of continuity management with the use of the CSF and KPI.

Desired Maturity Model

Managed and Measurable

Responsibilities and standards for continuous service are enforced. Responsibility for maintaining the continuous service plan is assigned. Maintenance activities take into account the changing business environment, the results of continuous service testing and best internal practices. Structured data about continuous service is being gathered, analysed, reported and acted upon. Training is provided for continuous service processes. System redundancy practices, including use of high-availability components, are being consistently deployed. Redundancy practices and continuous service planning influence each other. Discontinuity incidents are classified and the increasing escalation path for each is well known to all involved.

High-level Security Requirements

The following high-level 17799 mappings were made to DS4:

- 11.1 Aspects of business continuity management

Control Objectives

As per COBIT Mapping between COBIT version 3 and ISO 17799: 2000 document

DS4.1 IT Continuity Framework

IT management, in cooperation with business process owners, should establish a continuity framework that defines the roles, responsibilities and the risk-based approach/methodology to be adopted, and the rules and structures to document the continuity plan as well as the approval procedures.

17799 requirement(s):

- Responsibility for business continuity planning should be defined in the information security policy (4.1.3).
- A management process should be defined for business continuity that is not limited to IT but encompasses the whole organization. Key elements of business continuity management are listed. They include risks, their likelihood and potential business impacts, risk mitigation, definition of a business continuity strategy and detailed plans, tests and updates of the plan, and management responsibility (11.1.1).

- Business impacts should be assessed and all business processes considered. A plan should be developed, based on the results of the risk assessment (11.1.2).

DS4.2 IT Continuity Plan Strategy and Philosophy

Management should ensure that the IT continuity plan is in line with the overall business continuity plan, to ensure consistency. Furthermore, the IT continuity plan should take into account the IT long- and short-range plans, to ensure consistency.

17799 requirement(s):

- The business continuity plan is focused on minimizing impacts on business processes (11.1).
- The continuity strategy should reflect business objectives and priorities; the continuity plans should be aligned with the continuity strategy (11.1.1).

DS4.3 IT Continuity Plan Contents

IT management should ensure that a written plan is developed containing the following:

– Guidelines on how to use the continuity plan

– Emergency procedures to ensure the safety of all affected staff members

– Response procedures meant to bring the business back to the state it was in before the incident or disaster

– Recovery procedures meant to bring the business back to the state it was in before the incident or disaster

– Procedures to safeguard and reconstruct the home site

– Coordination procedures with public authorities

– Communication procedures with stakeholders, employees, key customers, critical suppliers, stockholders and management

– Critical information on continuity teams, affected staff, customers, suppliers, public authorities and media

17799 requirement(s):

- Content of the plan should be comparable to the requirements listed in DS4.3 (11.1.3).
- The planning framework should provide detailed guidance for developing and maintaining continuity plans (11.1.4).

DS4.4 Minimizing IT Continuity Requirements

IT management should establish procedures and guidelines for minimizing the continuity requirements with regard to personnel, facilities, hardware, software, equipment, forms, supplies and furniture.

17799 requirement(s):

- Local responsibilities for IT equipment and systems should be assigned (4.1.3).

DS4.5 Maintaining the IT Continuity Plan

IT management should provide for change control procedures to ensure that the continuity plan is up-to-date and reflects actual business requirements. This should require continuity plan maintenance procedures aligned with change, management and human resources procedures.

17799 requirement(s):

- Continuity plans should be maintained. Example situations that indicate the potential need to update the plan are listed in the ISO standard (11.1.5.2).

DS4.6 Testing the IT Continuity Plan

To have an effective continuity plan, management should assess its adequacy on a regular basis or upon major changes to the business or IT infrastructure. This requires careful preparation, documentation, reporting of test results and, according to the results, implementation of an action plan.

17799 requirement(s):

- Regular tests should be discussed. The testing should unveil incorrect assumptions or failures in the planning process or plan. Awareness is mentioned and techniques for tests are enumerated (e.g., test of supplier facilities, table-top testing) in the ISO standard (11.1.5.1).

DS4.7 IT Continuity Plan Training

The disaster continuity methodology should ensure that all concerned parties receive regular training regarding the procedures to be followed in case of an incident or disaster.

17799 requirement(s):

- Awareness and education should be a key component of the overall business continuity framework to ensure that the parties involved have the necessary training and continued understanding to perform their roles effectively (11.1.4).
- Simulation testing should be a component of the business continuity plan (BCP) test and maintenance strategy as well as a means to provide the training necessary to all parties involved (11.1.5.1).

DS4.8 IT Continuity Plan Distribution

Given the sensitive nature of information in the continuity plan, the latter should be distributed only to authorized personnel and should be safeguarded against unauthorized disclosure. Consequently, sections of the plan should be distributed on a need-to-know basis.

17799 requirement(s):

- Security considerations should be applied for continuity plans (7.1.3).

DS4.9 User Department Alternative Processing Backup Procedures

The continuity methodology should ensure that the user departments establish alternative processing procedures that may be used until the IT function is able to fully restore its services after a disaster or an event.

17799 requirement(s):

- The business continuity plan framework should have several components with specific ownership, such as emergency procedures, manual fallback plans and resumption plans, that are assigned to the owners of the appropriate business resources or processes (11.1.4).

DS4.10 Critical IT Resources

The continuity plan should identify the critical application programs, third-party services, operating systems, personnel and supplies, data files, and time frames needed for recovery after a disaster occurs. Critical data and operations should be identified, documented, prioritized and approved by the business process owners, in cooperation with IT management.

17799 requirement(s):

- Local responsibilities for IT equipment and systems should be assigned (4.1.3).
- The business continuity plan framework should have several components with specific ownership, such as emergency procedures, manual fallback plans and resumption plans that are assigned to the owners of the appropriate business resources or processes (11.1.4).

DS4.11 Backup Site and Hardware

Management should ensure that the continuity methodology incorporates an identification of alternatives regarding the backup site and hardware as well as a final alternative selection. If applicable, a formal contract for these types of services should be concluded.

17799 requirement(s):

- Physical protection should be adequate, even for backup site and hardware (7.2).
- Resources that are required for contingency should be identified (11.1.3).

DS4.12 Offsite Backup Storage

Offsite storage of critical backup media, documentation and other IT resources should be established to support recovery and business continuity plans. Business process owners and IT function personnel should be involved in determining what backup resources need to be stored offsite. The offsite storage facility should be environmentally appropriate to the media and other resources stored, and should have a level of security commensurate with that needed to protect the backup resources from unauthorized access, theft or damage. IT management should ensure that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security.

17799 requirement(s):

- Backup media should be stored at a safe distance (7.1.3).
- Physical protection of media stored offsite should be adequate and meet the requirements of the organization's physical security policy (7.2).

DS4.13 Wrap-up Procedures

On successful resumption of the IT function after a disaster, IT management should establish procedures for assessing the adequacy of the plan and update the plan accordingly.

17799 requirement(s):

- Not addressed in ISO/IEC17799

Critical Success Factors

- A no-break power system is installed and regularly tested
- Potential availability risks are proactively detected and addressed
- Critical infrastructure components are identified and continuously monitored
- Continuous service provision is a continuum of advance capacity planning, acquisition of high-availability components, needed redundancy, existence of tested contingency plans and the removal of single points of failure
- Action is taken on the lessons learned from actual downtime incidents and test executions of contingency plans
- Availability requirements analysis is performed regularly
- Service level agreements are used to raise awareness and increase co-operation with suppliers for continuity needs
- The escalation process is clearly understood and based on a classification of availability incidents
- The business costs of interrupted service are specified and quantified where possible, providing the motivation to develop appropriate plans and arrange for contingency facilities

Key Performance Indicators

- Number of outstanding continuous service issues not resolved or addressed
- Number and extent of breaches of continuous service, using duration and impact criteria
- Time lag between organisational change and continuity plan update
- Time to diagnose an incident and decide on continuity plan execution
- Time to normalise the service level after execution of the continuity plan
- Number of proactive availability fixes implemented
- Lead time to address continuous service shortfalls
- Frequency of continuous service training provided
- Frequency of continuous service testing

DS 5 – Ensure Systems Security

Safeguard information against unauthorized use, disclosure or modification, damage or loss

For the DS5 objective to be implemented successfully in the municipality, it needs to implement the detailed control objectives, as well as the corresponding ISO 17799 security controls, at a managed and measurable level by measuring its compliance against the critical success factors (CSF) and measuring performance against the key performance indicators (KPI).

In order to meet the Optimised governance level, the following steps are necessary:

1. Create awareness throughout the municipality that it is required to ensure the security of its IT systems.

2. Identify and define procedures in order to manage IT security of the municipality.

3. Document these procedures and assign the responsibility to perform them to the designated authority.

4. Manage and Monitor the process of IT security management with the use of the CSF and KPI.

5. Continually create efforts to benchmark the security to that of other institutions and refine the IT security function to that of best practice approaches.

Desired Maturity Model

Optimised

IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives. IT security requirements are clearly defined, optimised and included in a verified security plan. Security functions are integrated with applications at the design stage and end users are increasingly accountable for managing security. IT security reporting provides early warning of changing and emerging risk, using automated active monitoring approaches for critical systems. Incidents are promptly addressed with formalised incident response procedures supported by automated tools. Periodic security assessments evaluate the effectiveness of implementation of the security plan. Information on new threats and vulnerabilities is systematically collected and analysed, and adequate mitigating controls are promptly communicated and implemented. Intrusion testing, root cause analysis of security incidents and pro-active identification of risk is the basis for continuous improvements. Security processes and technologies are integrated organisation wide.

High-level Security Requirements

The following high-level 17799 mappings were made to DS5:

- 3.1 Information security policy
- 4.2 Security of third-party access
- 5.2 Information Classification
- 6.3 Responding to information security incidents and malfunctions
- 8.3 Protect against malicious software
- 8.5 Network management
- 9.1 Business requirement for access control
- 9.2 User access management
- 9.3 User responsibilities
- 9.4 Network access control
- 9.5 Operating system access control
- 9.6 Application access control
- 9.7 Monitoring system access and use
- 12.1 Compliance with legal requirements

Control Objectives

As per COBIT Mapping between COBIT version 3 and ISO 17799: 2000 document

DS5.1 Manage Security Measures

IT security should be managed such that security measures are in line with business requirements, including:

– Translating risk assessment information to the IT security plans

– Implementing the IT security plan

– Updating the IT security plan to reflect changes in the IT configuration

– Assessing the impact of change requests on IT security

– Monitoring the implementation of the IT security plan

– Aligning IT security procedures to other policies and procedures

17799 requirement(s):

- Management should issue a security policy (3.1).
- Documents that might support the security policy should be referenced (3.1.1).
- The information security forum should show support of information security (4.1.2).
- Physical security measures should be adequate to control identified risks (7.1).
- Recording information (e.g., by taking photos) should not be allowed (7.1.4).
- Procedures should be documented, and the documentation should be maintained (8.1.1).
- Media should be controlled and physically protected to prevent damage (8.6).
- Clear documentation should exist for procedures and authorization levels (8.6.1).
- Access to information should be controlled by adequate access restrictions and controls (9.1).
- An access security policy should be issued (9.1.1.1).
- User awareness should be facilitated, as it is important to maintain an effective level of security (9.3).
- Password use should be communicated to users (9.3.1).
- Network services and relevant controls should be documented in a policy (9.4.1).
- Access to application systems should be restricted to authorized users (9.6).
- Application-specific access policies should be compliant with the organizational information access policy (9.6.1).
- A policy for cryptographic controls should be issued (10.3.1).

DS5.2 Identification, Authentication and Access

The logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication and authorization mechanisms, linking users and resources with access rules. Such mechanisms should prevent unauthorized personnel, dial-up connections and other system (network) entry ports from accessing computer resources and minimize the need for authorized users to use multiple sign-ons. Procedures should also be in place to keep authentication and access mechanisms effective (e.g., regular password changes).

17799 requirement(s):

- Access of third parties should be controlled (4.2).
- Adequate privilege management should be included in application systems. Authorizations should be documented and follow a defined process (9.2.2).
- Passwords should be used for authentication. Passwords should be given to identified users in a secure manner and not in unprotected electronic mail messages (9.2.3).
- Access controls to internal and external networked services should be in place (9.4).
- User authentication for external connections should be controlled. Access restrictions should be based on a risk assessment. Authentication should consider hardware tokens, challenge/response protocols, dial-back or other mechanisms (9.4.3).
- Authentication mechanisms should be based on node authentication, if applicable (9.4.4).
- Access controls (e.g., key locks) should ensure that only required access can be obtained. This should include procedures and arrangements (9.4.5).
- Special access controls should be in place for shared networks (9.4.7).
- Identity should be verified as part of operation system access control. Identification of the user's location should be considered (9.5).
- Connection to specific locations should be based on automatic terminal identification, when appropriate (9.5.1).
- Requirements for terminal logon procedures (e.g., maximum number of unsuccessful logon attempts) provided in the ISO standard should be considered (9.5.2).

- A unique user ID should be required for all individuals. Users' privileges should not be identifiable by the user ID. A shared user ID should be used only when a clear business case exists. Identification and authentication can be based on passwords, biometric technologies or a combination of technologies (9.5.3).
- A good password management system raises the quality of passwords and should be implemented. Requirements for password management systems are provided in the ISO standard (9.5.4).
- Access should be ended after defined time-out delay. Alternatively, screen savers that prevent unauthorized access to terminals can be used (9.5.7).

DS5.3 Security of Online Access to Data

In an online IT environment, IT management should implement procedures in line with the security policy that provides access security control based on the individual's demonstrated need to view, add, change or delete data.

17799 requirement(s):

- Physical and logical access should be controlled (4.2.1.1).
- Access to data should be limited to authorized users and adequate protection should be implemented in application systems. Operating system software and other utility programs that could provide online access to data should be protected (9.6).

DS5.4 User Account Management

Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing user accounts. A formal approval procedure outlining the data or system owner granting the access privileges should be included. The security of third-party access should be defined contractually and address administration and nondisclosure requirements. Outsourcing arrangements should address the risks, security controls and procedures for information systems and networks in the contract between the parties.

17799 requirement(s):

- The reason for third-party access should be investigated and documented (4.2.1.2).
- Responsibility of managers should be clearly defined and include the definition and documentation of authorization levels (4.1.3).
- Authorization for the use of application systems should be documented and follow a defined authorization process (4.1.4).
- Personal circumstances of authorized staff should be monitored (6.1.2).
- Physical access authorization to information processing facilities should be maintained (7.1.2).
- Access restrictions should be valid even for security recovery procedures (8.1.3).
- Handling and storage of information should be controlled by access restrictions (8.6.3).
- Considerations for access control rules provided in the ISO standard should be considered (9.1.1.2).
- Formal procedures should control allocation of access rights. This procedure should cover issuing, altering, suspending and closing users' accounts. Privileged access rights should be tightly controlled (9.2).

- User registration should follow a formal procedure. Detailed controls to consider are enumerated in the ISO standard (9.2.1).
- Special privileges (e.g., use of tools that override application controls) should be controlled (9.2.2).
- Application systems should have adequate mechanisms (menus, different types of access, etc.) to restrict access to information (9.6.1).
- Access controls to system test data should reflect the productive environment (10.4.2).

DS5.5 Management Review of User Accounts

Management should have a control process in place to review and confirm access rights periodically. Periodic comparison of resources with recorded accountability should be made to help reduce the risk of errors, fraud, misuse or unauthorized alteration.

17799 requirement(s):

- Distribution lists should be reviewed regularly (8.6.3).
- Management should review user access rights on a regular basis. Privileged access rights should be monitored every three months (9.2.4).

DS5.6 User Control of User Accounts

Users should systematically control the activity of their proper account(s). Information mechanisms should be in place to allow them to oversee normal activity as well as to be alerted to unusual activity in a timely manner.

17799 requirement(s):

- Users should be aware of their responsibility for maintaining access controls (9.3).
- Information regarding the previous logon (successful and unsuccessful) should be provided after successful logon (9.5.2).

DS5.7 Security Surveillance

IT security administration should ensure that security activity is logged and any indication of imminent security violation is reported immediately to all who may be concerned, internally and externally, and is acted upon in a timely manner.

17799 requirement(s):

- The security policy should be reviewed regularly using recorded information, which is an important source for reviews (3.1.2).
- System access controls should include logging of security-relevant information (9.5).
- Terminal logon controls should include logging of unsuccessful logon attempts (9.5.2).
- A complete log of the use of system utilities should be maintained (9.5.5).
- Security incidents should be investigated, and evidence should be collected. Systems should be monitored and effectiveness of access controls should be verified (9.7).

- Audit logs should provide relevant information and log security-relevant events and security incidents (9.7.1).
- Based on a risk assessment, information to enable system monitoring should be defined. Details are provided in the ISO standard (9.7.2.1).
- A regular review of monitoring activities should be performed (9.7.2.2).
- Qualified personnel should perform log reviews, and further investigation should be performed, if required (9.7.2.3).
- Access to program source libraries should be logged (10.4.3).
- Computer misuse should be documented and logged (12.1.5).
- Logging security relevant activity should follow the rules for collection of evidence (12.1.7).

DS5.8 Data Classification

Management should implement procedures to ensure that all data are classified in terms of sensitivity by a formal and explicit decision by the data owner, and according to the data classification scheme. Even data needing "no protection" should require a formal decision to be so designated. Owners should determine disposition and sharing of data, as well as whether and when programs and files are to be maintained, archived or deleted. Evidence of owner approval and data disposition should be maintained. Policies should be defined to support reclassification of information based on changing sensitivities. The classification scheme should include criteria for managing exchanges of information between organizations, addressing both security and compliance with relevant legislation.

17799 requirement(s):

- Defined and documented authorization levels should be available (4.1.3).
- The classification of information should be based on a defined classification guideline. The level of information protection depends on clear classification of the information (5.2).
- Classified data should be labeled (5.2.1).
- The originator or a nominated owner of the information should be responsible for the classification (5.2.1).
- Access control rules should consider changes in information labels, as defined in the classification guidelines (9.1.1.2).
- Security requirements of systems should be based on agreed classifications (10.1).
- Organizational records (including different media) should be classified (12.1.3).

DS5.9 Central Identification and Access Rights Management

Controls should be in place to ensure that the identification and access rights of users and the identity of system and data owners are established and managed in a unique and central manner to obtain consistency and efficiency of global access control.

17799 requirement(s):

- Not addressed in ISO/IEC17799

DS5.10 Violation and Security Activity Reports

IT security administration should ensure that violation and security activity is logged, reported, reviewed and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorized activity. The logical access to the computer resources accountability information (security and other logs) should be granted based upon the principle of least privilege, or need to know.

17799 requirement(s):

- Security incidents should be reviewed and monitored by supervision of the management forum (4.1.1).
- The management information security forum should be responsible for reviews of information security incidents (4.1.2).
- Points of contact with qualified sources of information should be contacted, if required (4.1.5).
- Security incidents should be logged and investigated in a timely manner. Procedures for incident response should be documented (6.3).
- Following a formal procedure, all security incidents should be reported in a timely manner (6.3.1).
- Users should be made aware of their responsibility to report security weaknesses and their prohibition against testing the weaknesses (6.3.2).
- A general rule for granting access should be established—either the stronger "it is permitted unless expressly allowed," or the weaker "everything is allowed, unless expressly forbidden" (9.1.1.2).
- System access and use should be closely monitored, and security-relevant events should be logged to collect evidence (9.7).
- Audit logs and other information should be produced and archived as required. Audit logs should include user IDs, logon/off date and time, identification of the devices and other information (9.7.1).
- The frequency of reviews should depend on the risk of the system to be reviewed (9.7.2.2).
- Qualified personnel should perform log reviews, and further investigation should be performed, if required (9.7.2.3).
- Reviews of the security level should be performed regularly (12.2).

DS5.11 Incident Handling

Management should establish a computer security incident handling capability to address security incidents by providing a centralized platform with sufficient expertise and equipped with rapid and secure communication facilities. Incident management responsibilities and procedures should be established to ensure an appropriate, effective and timely response to security incidents.

17799 requirement(s):

- Incident recording should be a source of information for review and update of the security policy (3.1.2).
- The management information security forum should be responsible for reviewing and monitoring security incidents (4.1.1).
- Information security coordination should perform reviews of security incidents (4.1.2).
- Specialists should be contacted, if required (4.1.5).
- Contacts with relevant authorities, security groups and industry fora should be established (4.1.6).
- Incident response procedures should be formalized, documented and communicated (6.3).

- Incident management response procedures should be defined for timely and effective incident response. Controls that should be considered are enumerated (8.1.3).
- Responding to a duress alarm should be considered in the design of application system security controls (9.5.6).

DS5.12 Reaccreditation

Management should ensure that reaccreditation of security (e.g., through "tiger teams") is periodically performed to keep the formally approved security level and the acceptance of residual risk up-to-date.

17799 requirement(s):

- There should be a clear requirement to ensure that the update and maintenance of the security policy are endorsed by management based on ongoing risk assessments. Information security policy should be established and approved by suitable management. Contacts with external specialists should be established, and different parties should be participating (4.1).
- A selected individual should contact internal or external security specialists. This should ensure consistency (4.1.5).

DS5.13 Counterparty Trust

Organizational policy should ensure that control practices are implemented to verify the authenticity of the counterparty providing electronic instructions or transactions. This can be implemented through trusted exchange of passwords, tokens or cryptographic keys.

17799 requirement(s):

- Formalized agreements for information and software exchange should be established. Protection of sensitive items should be agreed upon (8.7.1).
- A comprehensive list of recommended controls to protect electronic commerce provided in the ISO standard should be considered (8.7.3).

DS5.14 Transaction Authorization

Organizational policy should ensure that, where appropriate, controls are implemented to provide authenticity of transactions and establish the validity of a user's claimed identity to the system. This requires use of cryptographic techniques for signing and verifying transactions.

17799 requirement(s):

- Detailed guidance on e-commerce transaction security requirements included in the ISO standard should be considered (8.7.3).
- The level of protection should be based on a risk assessment. If required, adequate cryptographic controls should be applied (10.3.2).

DS5.15 Non-repudiation

Organizational policy should ensure that, where appropriate, transactions cannot be denied by either party, and controls are implemented to provide non-repudiation of origin or receipt, proof of submission and receipt of transactions. This can be implemented through digital signatures, time stamping and trusted third parties, with appropriate policies that take into account relevant regulatory requirements.

17799 requirement(s):

- Messages should be protected against unauthorized modification and corruption by message authentication techniques (10.2.3).
- Digital signatures should protect authenticity and integrity of electronic documents. Appropriate controls should be applied (10.3.3).
- The use of non-repudiation services should be considered (10.3.4).

DS5.16 Trusted Path

Organizational policy should ensure that sensitive transaction data are exchanged only over a trusted path. Sensitive information includes security management information, sensitive transaction data, passwords and cryptographic keys. To achieve this, trusted channels may need to be established using encryption between users, between users and systems, and between systems.

17799 requirement(s):

- Information exchange over public networks should be controlled accordingly (8.5.1).
- An enforced path for transportation over networks should be considered. Controls to enforce a path are provided in the ISO standard (9.4.2).
- External connection should provide special controls such as specialized authentication methods for remote users (9.4.3).
- Routing controls should be considered in network controls (9.4.8).

DS5.17 Protection of Security Functions

All security-related hardware and software should be protected at all times against tampering to maintain their integrity and against disclosure of secret keys. In addition, organizations should keep a low profile about their security designs, but should not base their security on the design being secret.

17799 requirement(s):

- Security-relevant information (e.g., internal telephone books) should not be accessible to the public (7.1.3).
- System documentation should be protected closely (8.6.4).
- Private keys should be stored in secure locations (10.3.3.).

- Cryptographic keys should be protected against damage and modification. Private keys should be protected against disclosure (10.3.5.1).
- A key management system should be established and relevant procedures should be defined (10.3.5.2).

DS5.18 Cryptographic Key Management

Management should define and implement procedures and protocols to be used for generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorized disclosure. If a key is compromised, management should ensure that this information is propagated to any interested party through the use of certificate revocation lists or similar mechanisms.

17799 requirement(s):

- Policies should be established for usage of encryption technologies. Relevant legislation and restriction should be considered. If required, specialists and legal advice should be sought (10.3.2).
- Considerations for applying digital signatures are discussed (10.3.3).
- Key management should be based on a defined management system (10.3.5.1).
- Procedures should be defined for cryptographic key management. Requirements are enumerated in the ISO standard (10.3.5.2).

DS5.19 Malicious Software Prevention, Detection and Correction

Regarding malicious software, such as computer viruses or Trojan horses, management should establish a framework of adequate preventive, detective and corrective control measures, and occurrence response and reporting. Business and IT management should ensure that procedures are established across the organization to protect information systems and technology from computer viruses. Procedures should incorporate virus protection, detection, occurrence response and reporting.

17799 requirement(s):

- Security incident response procedures should be defined (6.3).
- Malicious software controls should be applied (8.3).
- Controls should consider detective and preventive controls. A list of examples is provided in the ISO standard (8.3.1).

DS5.20 Firewall Architectures and Connections with Public Networks

If connection to the Internet or other public networks exists, adequate firewalls should be operative to protect against denials of service and any unauthorized access to the internal resources, and control any application and infrastructure management flows in both directions.

17799 requirement(s):

- Networks should be controlled with adequate techniques. Boundaries to external networks should be established and maintained (8.5).
- Several controls to maintain security in networks discussed in the ISO standard should be considered (8.5.1).
- Networks should be segregated into several segments, if required (9.4.6).
- Access to network segments should be controlled (9.4.7).
- Access to public and private network services should be controlled (9.4.9).

DS5.21 Protection of Electronic Value

Management should protect the continued integrity of all cards or similar physical mechanisms used for authentication or storage of financial or other sensitive information, taking into consideration the related facilities, devices, employees and validation methods used.

17799 requirement(s):

- Information assets should be protected based on their classification (5.2).

Critical Success Factors

- An overall security plan is developed that covers the building of awareness, establishes clear policies and standards, identifies a cost-effective and sustainable implementation, and defines monitoring and enforcement processes
- There is awareness that a good security plan takes time to evolve
- The corporate security function reports to senior management and is responsible for executing the security plan
- Management and staff have a common understanding of security requirements, vulnerabilities and threats, and they understand and accept their own security responsibilities
- Third-party evaluation of security policy and architecture is conducted periodically
- A "building permit" programme is defined, identifying security baselines that have to be adhered to
- A "drivers license" programme is in place for those developing, implementing and using systems, enforcing security certification of staff
- The security function has the means and ability to detect, record, analyze significance, report and act upon security incidents when they do occur, while minimising the probability of occurrence by applying intrusion testing and active monitoring
- A centralised user management process and system provides the means to identify and assign authorisations to users in a standard and efficient manner
- A process is in place to authenticate users at reasonable cost, light to implement and easy to use

Key Performance Indicators

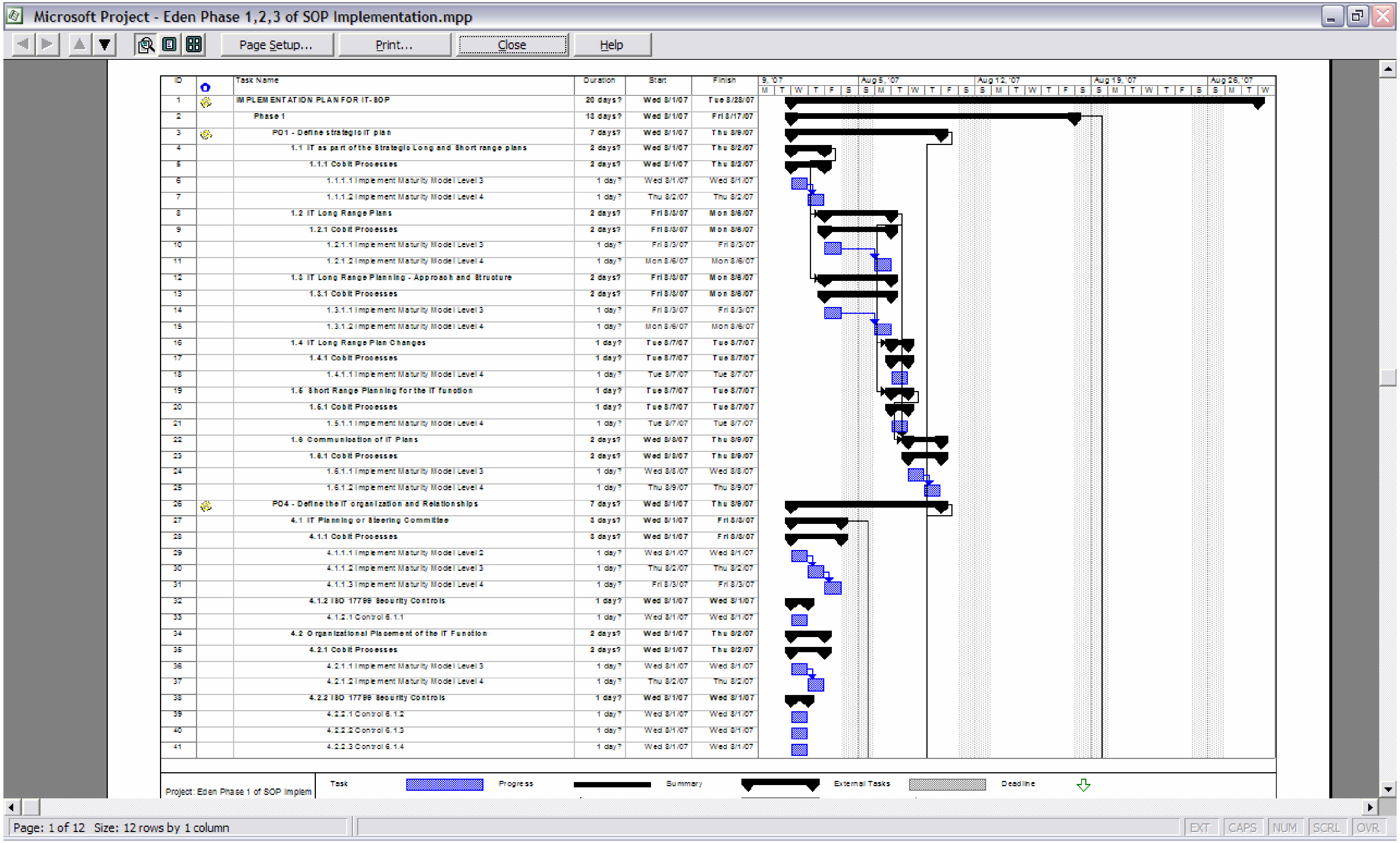
- Reduced number of security-related service calls, change requests and fixes
- Amount of downtime caused by security incidents
- Reduced turnaround time for security administration requests
- Number of systems subject to an intrusion detection process

- Number of systems with active monitoring capabilities
- Reduced time to investigate security incidents
- Time lag between detection, reporting and acting upon security incidents
- Number of IT security awareness training days

The IT-SOP's length is 180 pages and therefore, only Phase 1 (PO1, PO4, AI6, DS4, DS5) was added as an Appendix.

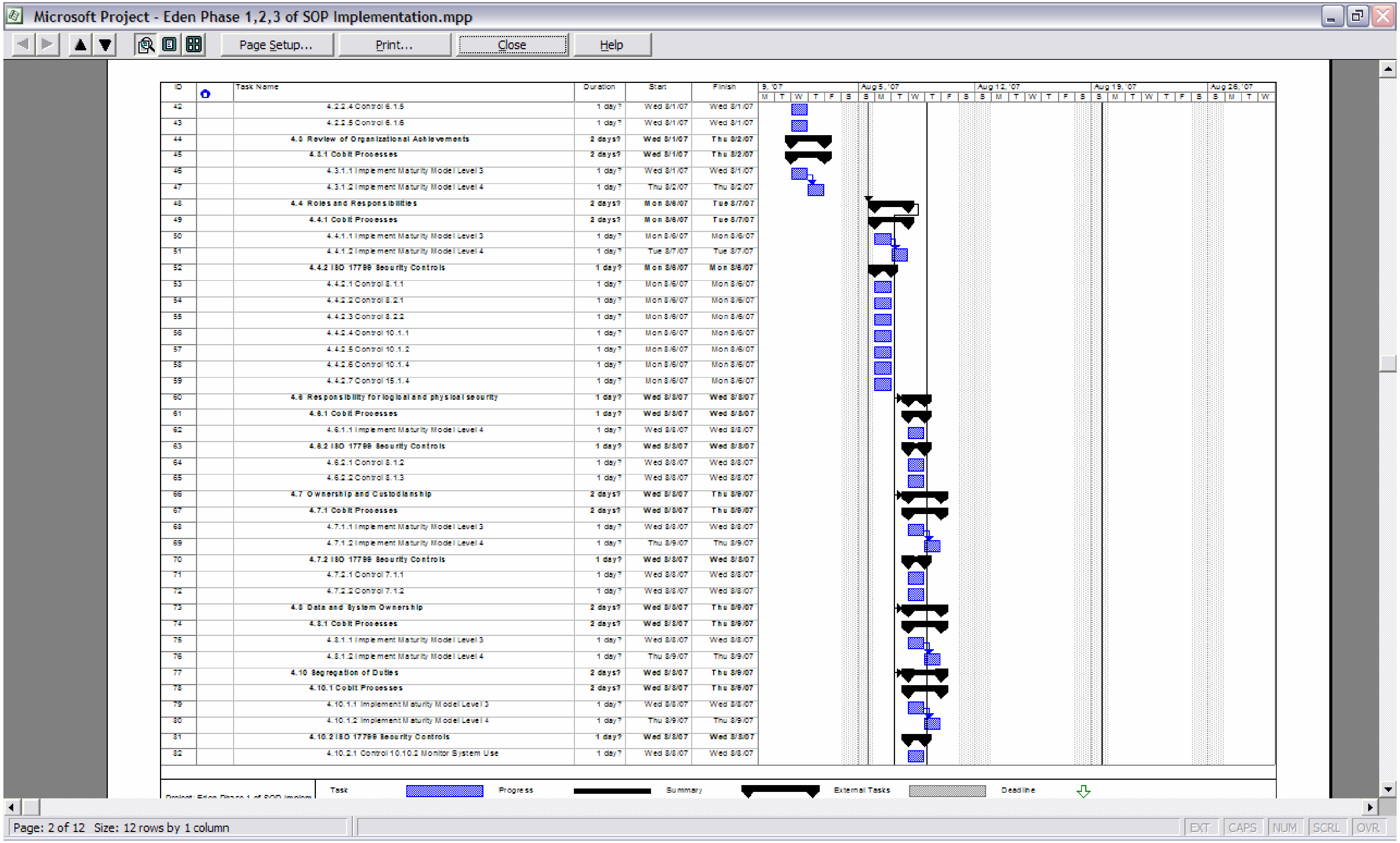
Appendix G

The Project Plan for the IT-SOP


Microsoft Project - Eden Phase 1,2,3 of SOP Implementation.mpp
Page Setup...
Print...
Close
Help
9, '07
Aug 5, '07
Aug 12, '07
Aug 19, '07
Aug 26, '07
M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W
Task
Progress
Summary
External Tasks
Deadline
Page: 1 of 12 Size: 12 rows by 1 column
EXT
CAPS
NUM
SCRL
OVR

ID		Task Name	Duration	Start	Finish
1		IMPLEMENTATION PLAN FOR IT-SOP	20 days?	Wed 8/1/07	Tue 8/28/07
2		Phase 1	13 days?	Wed 8/1/07	Fri 8/17/07
3		PO1 - Define strategic IT plan	7 days?	Wed 8/1/07	Thu 8/9/07
4		1.1 IT as part of the Strategic Long and Short range plans	2 days?	Wed 8/1/07	Thu 8/2/07
5		1.1.1 Cobit Processes	2 days?	Wed 8/1/07	Thu 8/2/07
6		1.1.1.1 Implement Maturity Model Level 3	1 day?	Wed 8/1/07	Wed 8/1/07
7		1.1.1.2 Implement Maturity Model Level 4	1 day?	Thu 8/2/07	Thu 8/2/07
8		1.2 IT Long Range Plans	2 days?	Fri 8/3/07	Mon 8/6/07
9		1.2.1 Cobit Processes	2 days?	Fri 8/3/07	Mon 8/6/07
10		1.2.1.1 Implement Maturity Model Level 3	1 day?	Fri 8/3/07	Fri 8/3/07
11		1.2.1.2 Implement Maturity Model Level 4	1 day?	Mon 8/6/07	Mon 8/6/07
12		1.3 IT Long Range Planning - Approach and Structure	2 days?	Fri 8/3/07	Mon 8/6/07
13		1.3.1 Cobit Processes	2 days?	Fri 8/3/07	Mon 8/6/07
14		1.3.1.1 Implement Maturity Model Level 3	1 day?	Fri 8/3/07	Fri 8/3/07
15		1.3.1.2 Implement Maturity Model Level 4	1 day?	Mon 8/6/07	Mon 8/6/07
16		1.4 IT Long Range Plan Changes	1 day?	Tue 8/7/07	Tue 8/7/07
17		1.4.1 Cobit Processes	1 day?	Tue 8/7/07	Tue 8/7/07
18		1.4.1.1 Implement Maturity Model Level 4	1 day?	Tue 8/7/07	Tue 8/7/07
19		1.5 Short Range Planning for the IT function	1 day?	Tue 8/7/07	Tue 8/7/07
20		1.5.1 Cobit Processes	1 day?	Tue 8/7/07	Tue 8/7/07
21		1.5.1.1 Implement Maturity Model Level 4	1 day?	Tue 8/7/07	Tue 8/7/07
22		1.6 Communication of IT Plans	2 days?	Wed 8/8/07	Thu 8/9/07
23		1.6.1 Cobit Processes	2 days?	Wed 8/8/07	Thu 8/9/07
24		1.6.1.1 Implement Maturity Model Level 3	1 day?	Wed 8/8/07	Wed 8/8/07
25		1.6.1.2 Implement Maturity Model Level 4	1 day?	Thu 8/9/07	Thu 8/9/07
26		PO4 - Define the IT organization and Relationships	7 days?	Wed 8/1/07	Thu 8/9/07
27		4.1 IT Planning or Steering Committee	3 days?	Wed 8/1/07	Fri 8/3/07
28		4.1.1 Cobit Processes	3 days?	Wed 8/1/07	Fri 8/3/07
29		4.1.1.1 Implement Maturity Model Level 2	1 day?	Wed 8/1/07	Wed 8/1/07
30		4.1.1.2 Implement Maturity Model Level 3	1 day?	Thu 8/2/07	Thu 8/2/07
31		4.1.1.3 Implement Maturity Model Level 4	1 day?	Fri 8/3/07	Fri 8/3/07
32		4.1.2 ISO 17799 Security Controls	1 day?	Wed 8/1/07	Wed 8/1/07
33		4.1.2.1 Control 6.1.1	1 day?	Wed 8/1/07	Wed 8/1/07
34		4.2 Organizational Placement of the IT Function	2 days?	Wed 8/1/07	Thu 8/2/07
35		4.2.1 Cobit Processes	2 days?	Wed 8/1/07	Thu 8/2/07
36		4.2.1.1 Implement Maturity Model Level 3	1 day?	Wed 8/1/07	Wed 8/1/07
37		4.2.1.2 Implement Maturity Model Level 4	1 day?	Thu 8/2/07	Thu 8/2/07
38		4.2.2 ISO 17799 Security Controls	1 day?	Wed 8/1/07	Wed 8/1/07
39		4.2.2.1 Control 6.1.2	1 day?	Wed 8/1/07	Wed 8/1/07
40		4.2.2.2 Control 6.1.3	1 day?	Wed 8/1/07	Wed 8/1/07
41		4.2.2.3 Control 6.1.4	1 day?	Wed 8/1/07	Wed 8/1/07

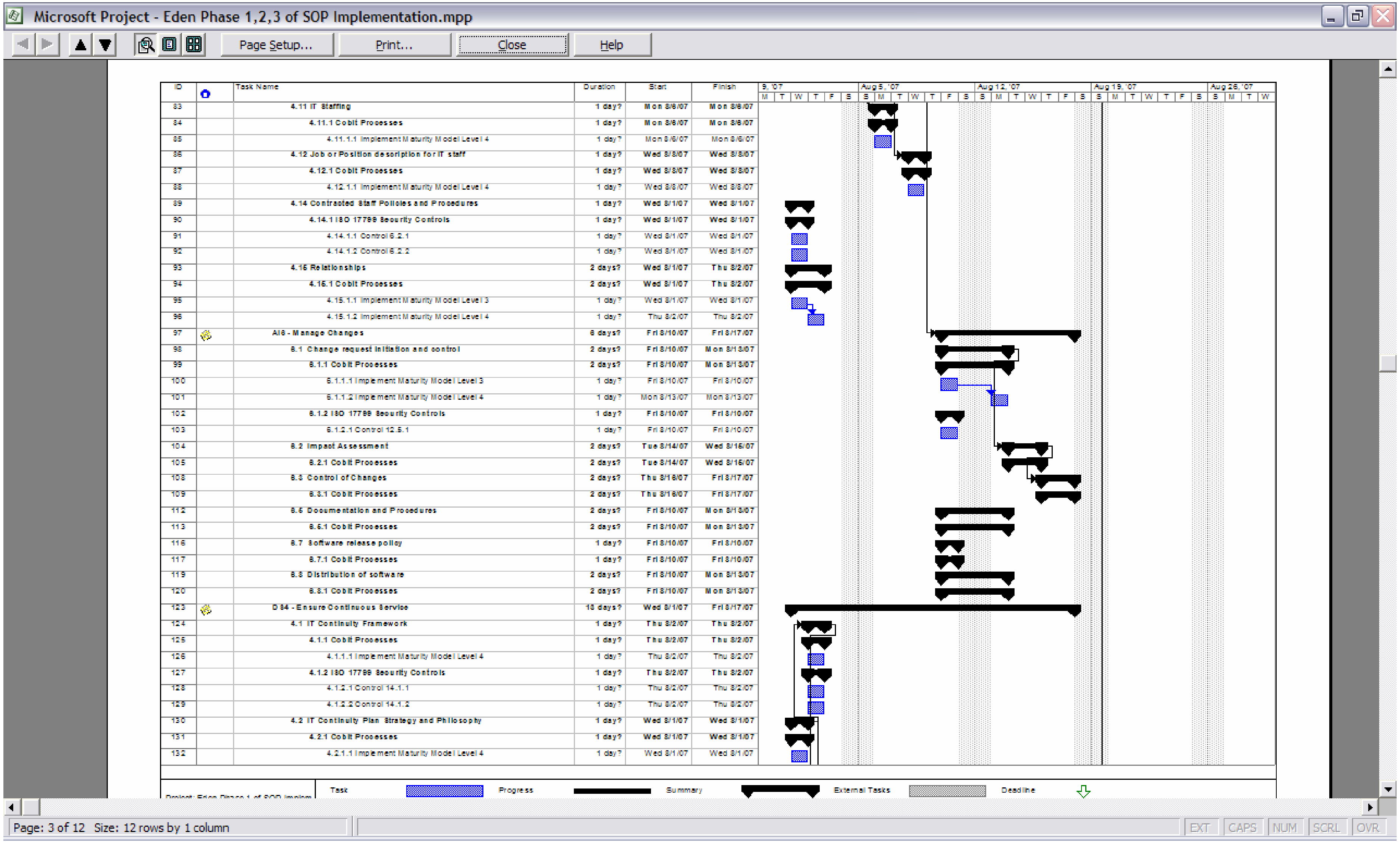
Project: Eden Phase 1 of SOP Implem



Microsoft Project - Eden Phase 1,2,3 of SOP Implementation.mpp
Page Setup...
Print...
Close
Help
9, '07
Aug 5, '07
Aug 12, '07
Aug 19, '07
Aug 26, '07
M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W
Task
Progress
Summary
External Tasks
Deadline
Project: Eden Phase 1 of SOP Implem
EXT
CAPS
NUM
SCRL
OVR

ID		Task Name	Duration	Start	Finish
42		4.2.2.4 Control 6.1.5	1 day?	Wed 8/1/07	Wed 8/1/07
43		4.2.2.5 Control 6.1.6	1 day?	Wed 8/1/07	Wed 8/1/07
44		**4.3 Review of Organizational Achievements**	**2 days?**	**Wed 8/1/07**	**Thu 8/2/07**
45		**4.3.1 Cobit Processes**	**2 days?**	**Wed 8/1/07**	**Thu 8/2/07**
46		4.3.1.1 Implement Maturity Model Level 3	1 day?	Wed 8/1/07	Wed 8/1/07
47		4.3.1.2 Implement Maturity Model Level 4	1 day?	Thu 8/2/07	Thu 8/2/07
48		**4.4 Roles and Responsibilities**	**2 days?**	**Mon 8/6/07**	**Tue 8/7/07**
49		**4.4.1 Cobit Processes**	**2 days?**	**Mon 8/6/07**	**Tue 8/7/07**
50		4.4.1.1 Implement Maturity Model Level 3	1 day?	Mon 8/6/07	Mon 8/6/07
51		4.4.1.2 Implement Maturity Model Level 4	1 day?	Tue 8/7/07	Tue 8/7/07
52		**4.4.2 ISO 17799 Security Controls**	**1 day?**	**Mon 8/6/07**	**Mon 8/6/07**
53		4.4.2.1 Control 8.1.1	1 day?	Mon 8/6/07	Mon 8/6/07
54		4.4.2.2 Control 8.2.1	1 day?	Mon 8/6/07	Mon 8/6/07
55		4.4.2.3 Control 8.2.2	1 day?	Mon 8/6/07	Mon 8/6/07
56		4.4.2.4 Control 10.1.1	1 day?	Mon 8/6/07	Mon 8/6/07
57		4.4.2.5 Control 10.1.2	1 day?	Mon 8/6/07	Mon 8/6/07
58		4.4.2.6 Control 10.1.4	1 day?	Mon 8/6/07	Mon 8/6/07
59		4.4.2.7 Control 15.1.4	1 day?	Mon 8/6/07	Mon 8/6/07
60		**4.6 Responsibility for logical and physical security**	**1 day?**	**Wed 8/8/07**	**Wed 8/8/07**
61		**4.6.1 Cobit Processes**	**1 day?**	**Wed 8/8/07**	**Wed 8/8/07**
62		4.6.1.1 Implement Maturity Model Level 4	1 day?	Wed 8/8/07	Wed 8/8/07
63		**4.6.2 ISO 17799 Security Controls**	**1 day?**	**Wed 8/8/07**	**Wed 8/8/07**
64		4.6.2.1 Control 8.1.2	1 day?	Wed 8/8/07	Wed 8/8/07
65		4.6.2.2 Control 8.1.3	1 day?	Wed 8/8/07	Wed 8/8/07
66		**4.7 Ownership and Custodianship**	**2 days?**	**Wed 8/8/07**	**Thu 8/9/07**
67		**4.7.1 Cobit Processes**	**2 days?**	**Wed 8/8/07**	**Thu 8/9/07**
68		4.7.1.1 Implement Maturity Model Level 3	1 day?	Wed 8/8/07	Wed 8/8/07
69		4.7.1.2 Implement Maturity Model Level 4	1 day?	Thu 8/9/07	Thu 8/9/07
70		**4.7.2 ISO 17799 Security Controls**	**1 day?**	**Wed 8/8/07**	**Wed 8/8/07**
71		4.7.2.1 Control 7.1.1	1 day?	Wed 8/8/07	Wed 8/8/07
72		4.7.2.2 Control 7.1.2	1 day?	Wed 8/8/07	Wed 8/8/07
73		**4.8 Data and System Ownership**	**2 days?**	**Wed 8/8/07**	**Thu 8/9/07**
74		**4.8.1 Cobit Processes**	**2 days?**	**Wed 8/8/07**	**Thu 8/9/07**
75		4.8.1.1 Implement Maturity Model Level 3	1 day?	Wed 8/8/07	Wed 8/8/07
76		4.8.1.2 Implement Maturity Model Level 4	1 day?	Thu 8/9/07	Thu 8/9/07
77		**4.10 Segregation of Duties**	**2 days?**	**Wed 8/8/07**	**Thu 8/9/07**
78		**4.10.1 Cobit Processes**	**2 days?**	**Wed 8/8/07**	**Thu 8/9/07**
79		4.10.1.1 Implement Maturity Model Level 3	1 day?	Wed 8/8/07	Wed 8/8/07
80		4.10.1.2 Implement Maturity Model Level 4	1 day?	Thu 8/9/07	Thu 8/9/07
81		**4.10.2 ISO 17799 Security Controls**	**1 day?**	**Wed 8/8/07**	**Wed 8/8/07**
82		4.10.2.1 Control 10.10.2 Monitor System Use	1 day?	Wed 8/8/07	Wed 8/8/07

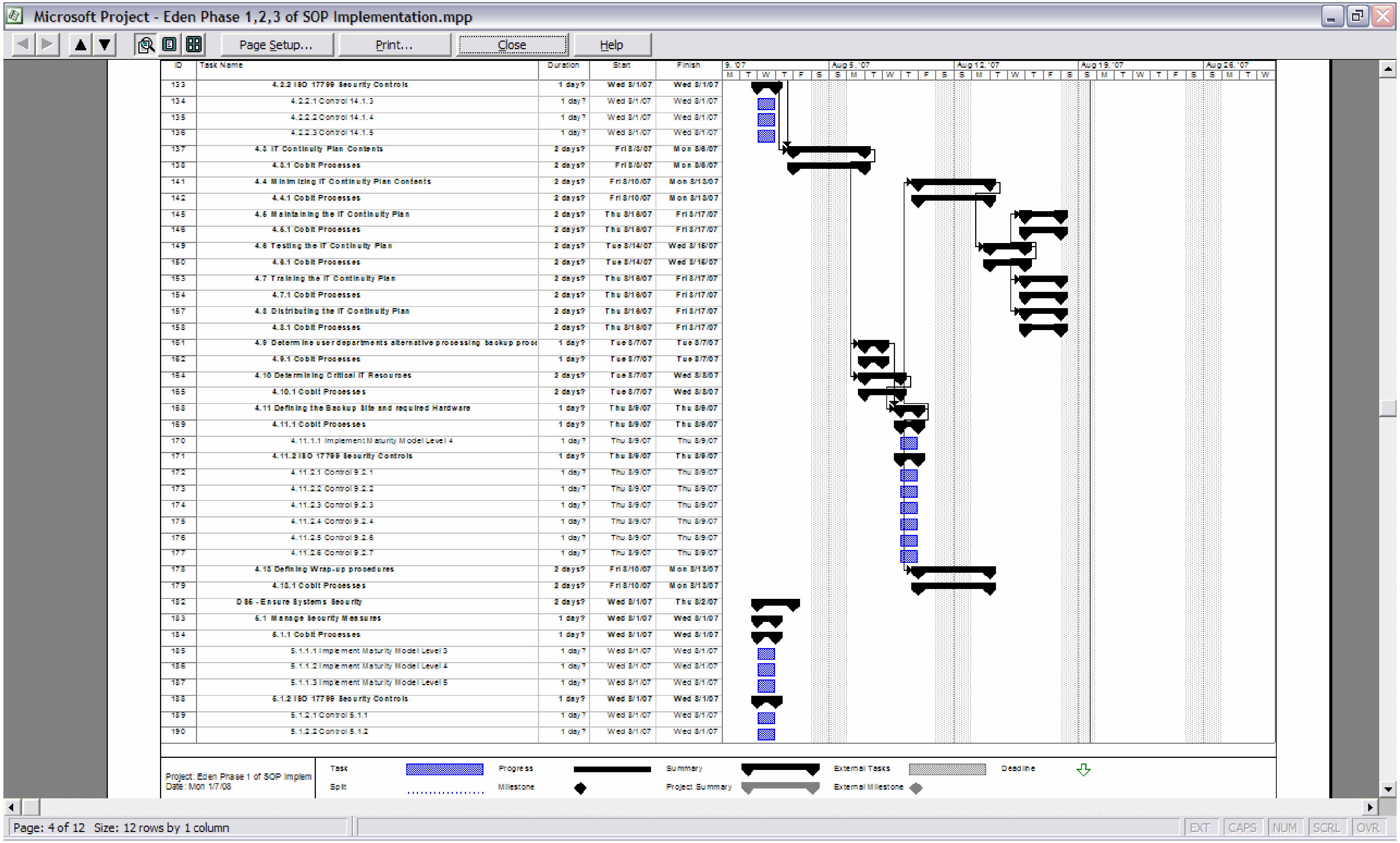
Page: 2 of 12 Size: 12 rows by 1 column



ID		Task Name	Duration	Start	Finish
83		4.11 IT Staffing	1 day?	Mon 8/6/07	Mon 8/6/07
84		4.11.1 Cobit Processes	1 day?	Mon 8/6/07	Mon 8/6/07
85		4.11.1.1 Implement Maturity Model Level 4	1 day?	Mon 8/6/07	Mon 8/6/07
86		4.12 Job or Position description for IT staff	1 day?	Wed 8/8/07	Wed 8/8/07
87		4.12.1 Cobit Processes	1 day?	Wed 8/8/07	Wed 8/8/07
88		4.12.1.1 Implement Maturity Model Level 4	1 day?	Wed 8/8/07	Wed 8/8/07
89		4.14 Contracted Staff Policies and Procedures	1 day?	Wed 8/1/07	Wed 8/1/07
90		4.14.1 ISO 17799 Security Controls	1 day?	Wed 8/1/07	Wed 8/1/07
91		4.14.1.1 Control 6.2.1	1 day?	Wed 8/1/07	Wed 8/1/07
92		4.14.1.2 Control 6.2.2	1 day?	Wed 8/1/07	Wed 8/1/07
93		4.15 Relationships	2 days?	Wed 8/1/07	Thu 8/2/07
94		4.15.1 Cobit Processes	2 days?	Wed 8/1/07	Thu 8/2/07
95		4.15.1.1 Implement Maturity Model Level 3	1 day?	Wed 8/1/07	Wed 8/1/07
96		4.15.1.2 Implement Maturity Model Level 4	1 day?	Thu 8/2/07	Thu 8/2/07
97		AI6 - Manage Changes	6 days?	Fri 8/10/07	Fri 8/17/07
98		6.1 Change request initiation and control	2 days?	Fri 8/10/07	Mon 8/13/07
99		6.1.1 Cobit Processes	2 days?	Fri 8/10/07	Mon 8/13/07
100		6.1.1.1 Implement Maturity Model Level 3	1 day?	Fri 8/10/07	Fri 8/10/07
101		6.1.1.2 Implement Maturity Model Level 4	1 day?	Mon 8/13/07	Mon 8/13/07
102		6.1.2 ISO 17799 Security Controls	1 day?	Fri 8/10/07	Fri 8/10/07
103		6.1.2.1 Control 12.5.1	1 day?	Fri 8/10/07	Fri 8/10/07
104		6.2 Impact Assessment	2 days?	Tue 8/14/07	Wed 8/15/07
105		6.2.1 Cobit Processes	2 days?	Tue 8/14/07	Wed 8/15/07
108		6.3 Control of Changes	2 days?	Thu 8/16/07	Fri 8/17/07
109		6.3.1 Cobit Processes	2 days?	Thu 8/16/07	Fri 8/17/07
112		6.5 Documentation and Procedures	2 days?	Fri 8/10/07	Mon 8/13/07
113		6.5.1 Cobit Processes	2 days?	Fri 8/10/07	Mon 8/13/07
116		6.7 Software release policy	1 day?	Fri 8/10/07	Fri 8/10/07
117		6.7.1 Cobit Processes	1 day?	Fri 8/10/07	Fri 8/10/07
119		6.8 Distribution of software	2 days?	Fri 8/10/07	Mon 8/13/07
120		6.8.1 Cobit Processes	2 days?	Fri 8/10/07	Mon 8/13/07
123		DS4 - Ensure Continuous Service	13 days?	Wed 8/1/07	Fri 8/17/07
124		4.1 IT Continuity Framework	1 day?	Thu 8/2/07	Thu 8/2/07
125		4.1.1 Cobit Processes	1 day?	Thu 8/2/07	Thu 8/2/07
126		4.1.1.1 Implement Maturity Model Level 4	1 day?	Thu 8/2/07	Thu 8/2/07
127		4.1.2 ISO 17799 Security Controls	1 day?	Thu 8/2/07	Thu 8/2/07
128		4.1.2.1 Control 14.1.1	1 day?	Thu 8/2/07	Thu 8/2/07
129		4.1.2.2 Control 14.1.2	1 day?	Thu 8/2/07	Thu 8/2/07
130		4.2 IT Continuity Plan Strategy and Philosophy	1 day?	Wed 8/1/07	Wed 8/1/07
131		4.2.1 Cobit Processes	1 day?	Wed 8/1/07	Wed 8/1/07
132		4.2.1.1 Implement Maturity Model Level 4	1 day?	Wed 8/1/07	Wed 8/1/07

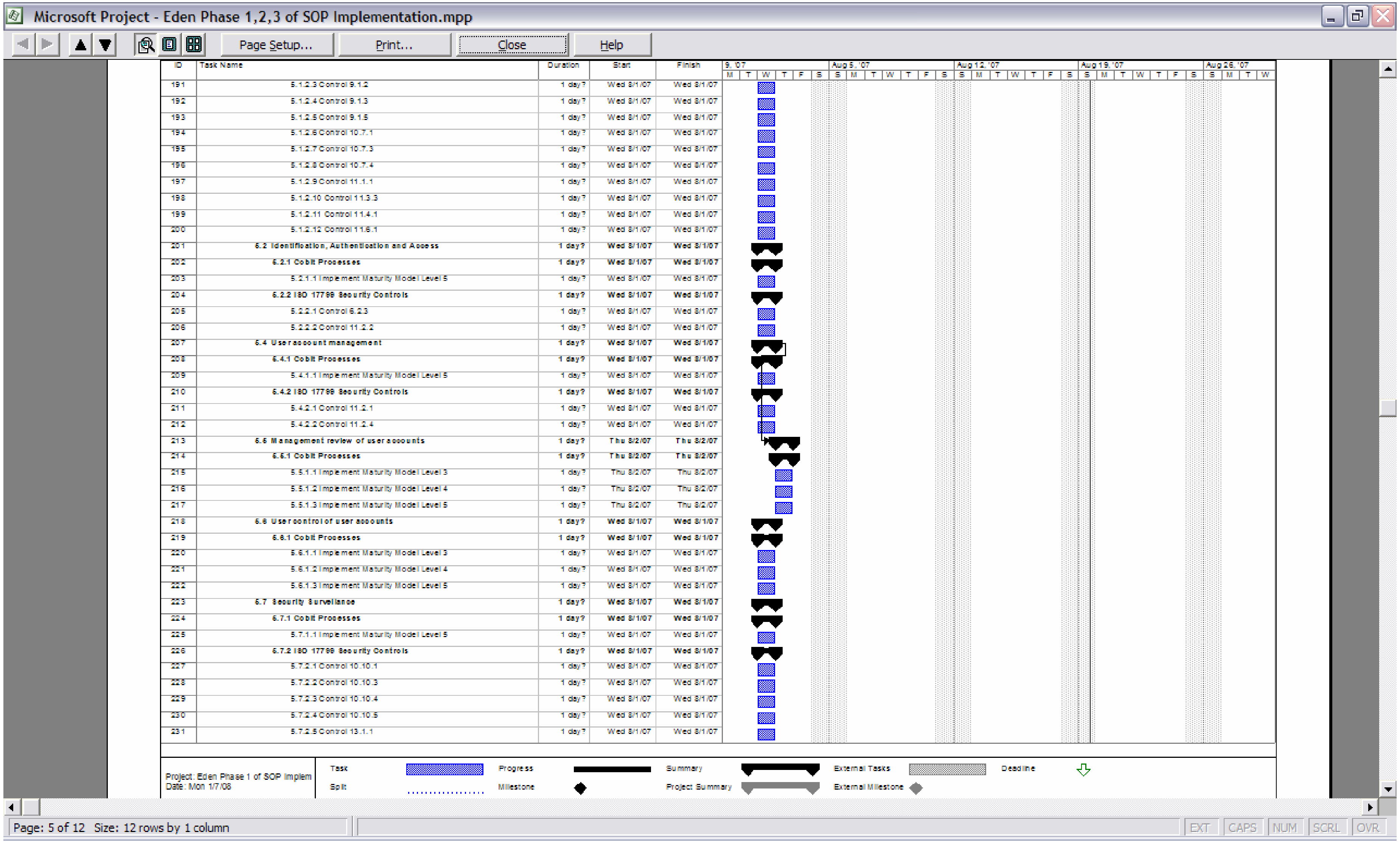
Project: Eden Phase 1 of SOP Implem

Page: 3 of 12 Size: 12 rows by 1 column



ID	Task Name	Duration	Start	Finish
133	4.2.2 ISO 17799 Security Controls	1 day?	Wed 8/1/07	Wed 8/1/07
134	4.2.2.1 Control 14.1.3	1 day?	Wed 8/1/07	Wed 8/1/07
135	4.2.2.2 Control 14.1.4	1 day?	Wed 8/1/07	Wed 8/1/07
136	4.2.2.3 Control 14.1.5	1 day?	Wed 8/1/07	Wed 8/1/07
137	4.3 IT Continuity Plan Contents	2 days?	Fri 8/3/07	Mon 8/6/07
138	4.3.1 Cobit Processes	2 days?	Fri 8/3/07	Mon 8/6/07
141	4.4 Minimizing IT Continuity Plan Contents	2 days?	Fri 8/10/07	Mon 8/13/07
142	4.4.1 Cobit Processes	2 days?	Fri 8/10/07	Mon 8/13/07
145	4.5 Maintaining the IT Continuity Plan	2 days?	Thu 8/16/07	Fri 8/17/07
146	4.5.1 Cobit Processes	2 days?	Thu 8/16/07	Fri 8/17/07
149	4.6 Testing the IT Continuity Plan	2 days?	Tue 8/14/07	Wed 8/15/07
150	4.6.1 Cobit Processes	2 days?	Tue 8/14/07	Wed 8/15/07
153	4.7 Training the IT Continuity Plan	2 days?	Thu 8/16/07	Fri 8/17/07
154	4.7.1 Cobit Processes	2 days?	Thu 8/16/07	Fri 8/17/07
157	4.8 Distributing the IT Continuity Plan	2 days?	Thu 8/16/07	Fri 8/17/07
158	4.8.1 Cobit Processes	2 days?	Thu 8/16/07	Fri 8/17/07
161	4.9 Determine user departments alternative processing backup proc	1 day?	Tue 8/7/07	Tue 8/7/07
162	4.9.1 Cobit Processes	1 day?	Tue 8/7/07	Tue 8/7/07
164	4.10 Determining Critical IT Resources	2 days?	Tue 8/7/07	Wed 8/8/07
165	4.10.1 Cobit Processes	2 days?	Tue 8/7/07	Wed 8/8/07
168	4.11 Defining the Backup Site and required Hardware	1 day?	Thu 8/9/07	Thu 8/9/07
169	4.11.1 Cobit Processes	1 day?	Thu 8/9/07	Thu 8/9/07
170	4.11.1.1 Implement Maturity Model Level 4	1 day?	Thu 8/9/07	Thu 8/9/07
171	4.11.2 ISO 17799 Security Controls	1 day?	Thu 8/9/07	Thu 8/9/07
172	4.11.2.1 Control 9.2.1	1 day?	Thu 8/9/07	Thu 8/9/07
173	4.11.2.2 Control 9.2.2	1 day?	Thu 8/9/07	Thu 8/9/07
174	4.11.2.3 Control 9.2.3	1 day?	Thu 8/9/07	Thu 8/9/07
175	4.11.2.4 Control 9.2.4	1 day?	Thu 8/9/07	Thu 8/9/07
176	4.11.2.5 Control 9.2.6	1 day?	Thu 8/9/07	Thu 8/9/07
177	4.11.2.6 Control 9.2.7	1 day?	Thu 8/9/07	Thu 8/9/07
178	4.13 Defining Wrap-up procedures	2 days?	Fri 8/10/07	Mon 8/13/07
179	4.13.1 Cobit Processes	2 days?	Fri 8/10/07	Mon 8/13/07
182	DS5 - Ensure Systems Security	2 days?	Wed 8/1/07	Thu 8/2/07
183	5.1 Manage Security Measures	1 day?	Wed 8/1/07	Wed 8/1/07
184	5.1.1 Cobit Processes	1 day?	Wed 8/1/07	Wed 8/1/07
185	5.1.1.1 Implement Maturity Model Level 3	1 day?	Wed 8/1/07	Wed 8/1/07
186	5.1.1.2 Implement Maturity Model Level 4	1 day?	Wed 8/1/07	Wed 8/1/07
187	5.1.1.3 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07
188	5.1.2 ISO 17799 Security Controls	1 day?	Wed 8/1/07	Wed 8/1/07
189	5.1.2.1 Control 5.1.1	1 day?	Wed 8/1/07	Wed 8/1/07
190	5.1.2.2 Control 5.1.2	1 day?	Wed 8/1/07	Wed 8/1/07

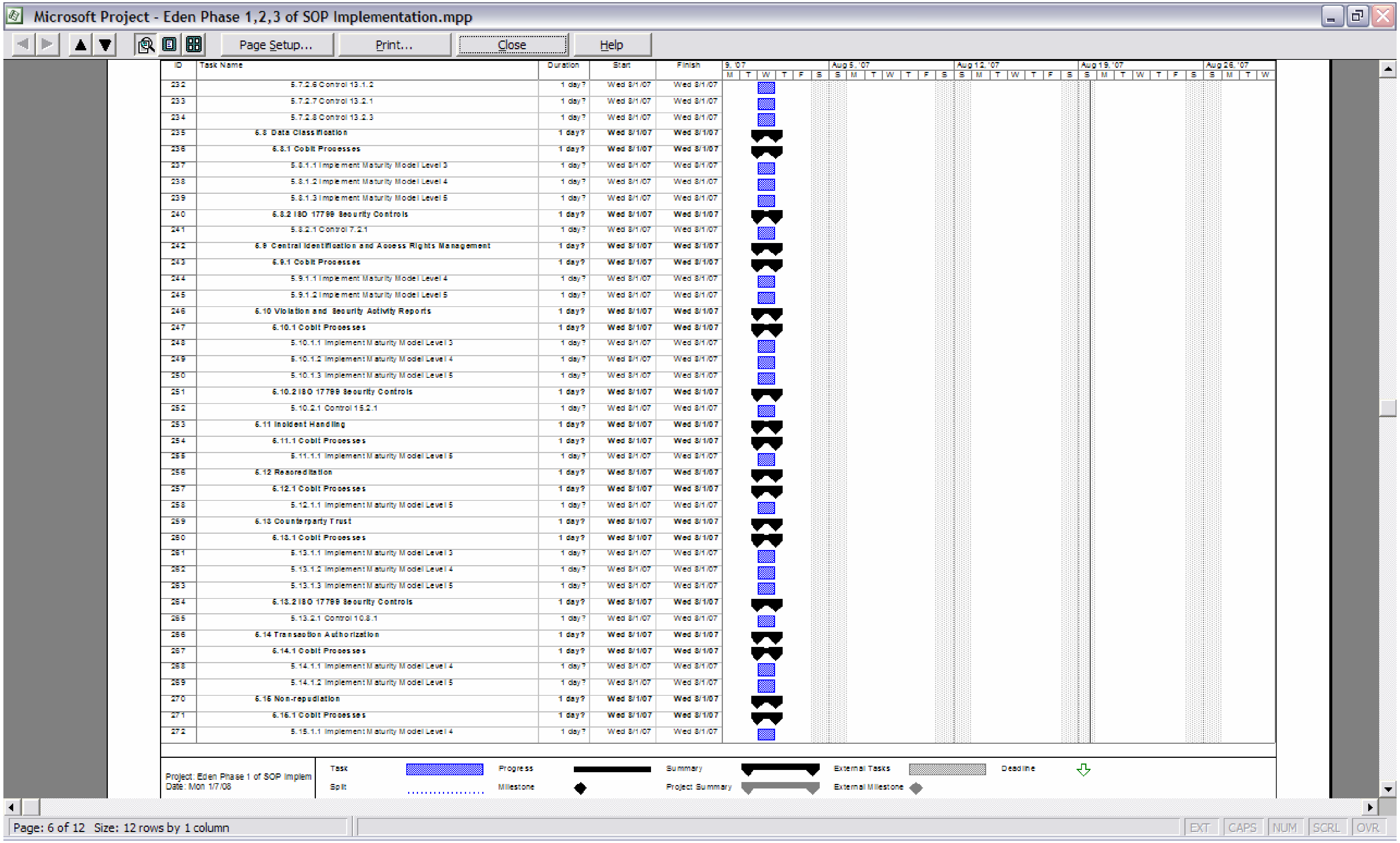
Project: Eden Phase 1 of SOP Implem
Date: Mon 1/7/08


Microsoft Project - Eden Phase 1,2,3 of SOP Implementation.mpp
Page Setup...
Print...
Close
Help
9, '07
Aug 5, '07
Aug 12, '07
Aug 19, '07
Aug 26, '07
M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W
Page: 5 of 12 Size: 12 rows by 1 column
EXT
CAPS
NUM
SCRL
OVR

ID	Task Name	Duration	Start	Finish
191	5.1.2.3 Control 9.1.2	1 day?	Wed 8/1/07	Wed 8/1/07
192	5.1.2.4 Control 9.1.3	1 day?	Wed 8/1/07	Wed 8/1/07
193	5.1.2.5 Control 9.1.5	1 day?	Wed 8/1/07	Wed 8/1/07
194	5.1.2.6 Control 10.7.1	1 day?	Wed 8/1/07	Wed 8/1/07
195	5.1.2.7 Control 10.7.3	1 day?	Wed 8/1/07	Wed 8/1/07
196	5.1.2.8 Control 10.7.4	1 day?	Wed 8/1/07	Wed 8/1/07
197	5.1.2.9 Control 11.1.1	1 day?	Wed 8/1/07	Wed 8/1/07
198	5.1.2.10 Control 11.3.3	1 day?	Wed 8/1/07	Wed 8/1/07
199	5.1.2.11 Control 11.4.1	1 day?	Wed 8/1/07	Wed 8/1/07
200	5.1.2.12 Control 11.6.1	1 day?	Wed 8/1/07	Wed 8/1/07
201	**5.2 Identification, Authentication and Access**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
202	**5.2.1 Cobit Processes**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
203	5.2.1.1 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07
204	**5.2.2 ISO 17799 Security Controls**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
205	5.2.2.1 Control 6.2.3	1 day?	Wed 8/1/07	Wed 8/1/07
206	5.2.2.2 Control 11.2.2	1 day?	Wed 8/1/07	Wed 8/1/07
207	**5.4 User account management**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
208	**5.4.1 Cobit Processes**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
209	5.4.1.1 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07
210	**5.4.2 ISO 17799 Security Controls**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
211	5.4.2.1 Control 11.2.1	1 day?	Wed 8/1/07	Wed 8/1/07
212	5.4.2.2 Control 11.2.4	1 day?	Wed 8/1/07	Wed 8/1/07
213	**5.5 Management review of user accounts**	**1 day?**	**Thu 8/2/07**	**Thu 8/2/07**
214	**5.5.1 Cobit Processes**	**1 day?**	**Thu 8/2/07**	**Thu 8/2/07**
215	5.5.1.1 Implement Maturity Model Level 3	1 day?	Thu 8/2/07	Thu 8/2/07
216	5.5.1.2 Implement Maturity Model Level 4	1 day?	Thu 8/2/07	Thu 8/2/07
217	5.5.1.3 Implement Maturity Model Level 5	1 day?	Thu 8/2/07	Thu 8/2/07
218	**5.6 User control of user accounts**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
219	**5.6.1 Cobit Processes**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
220	5.6.1.1 Implement Maturity Model Level 3	1 day?	Wed 8/1/07	Wed 8/1/07
221	5.6.1.2 Implement Maturity Model Level 4	1 day?	Wed 8/1/07	Wed 8/1/07
222	5.6.1.3 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07
223	**5.7 Security Surveillance**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
224	**5.7.1 Cobit Processes**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
225	5.7.1.1 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07
226	**5.7.2 ISO 17799 Security Controls**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
227	5.7.2.1 Control 10.10.1	1 day?	Wed 8/1/07	Wed 8/1/07
228	5.7.2.2 Control 10.10.3	1 day?	Wed 8/1/07	Wed 8/1/07
229	5.7.2.3 Control 10.10.4	1 day?	Wed 8/1/07	Wed 8/1/07
230	5.7.2.4 Control 10.10.5	1 day?	Wed 8/1/07	Wed 8/1/07
231	5.7.2.5 Control 13.1.1	1 day?	Wed 8/1/07	Wed 8/1/07

Project: Eden Phase 1 of SOP Implem
Date: Mon 1/7/08

Task	▨	Progress	▬	Summary	▬	External Tasks	▨	Deadline	⇩
Split	....	Milestone	◆	Project Summary	▬	External Milestone	◆		

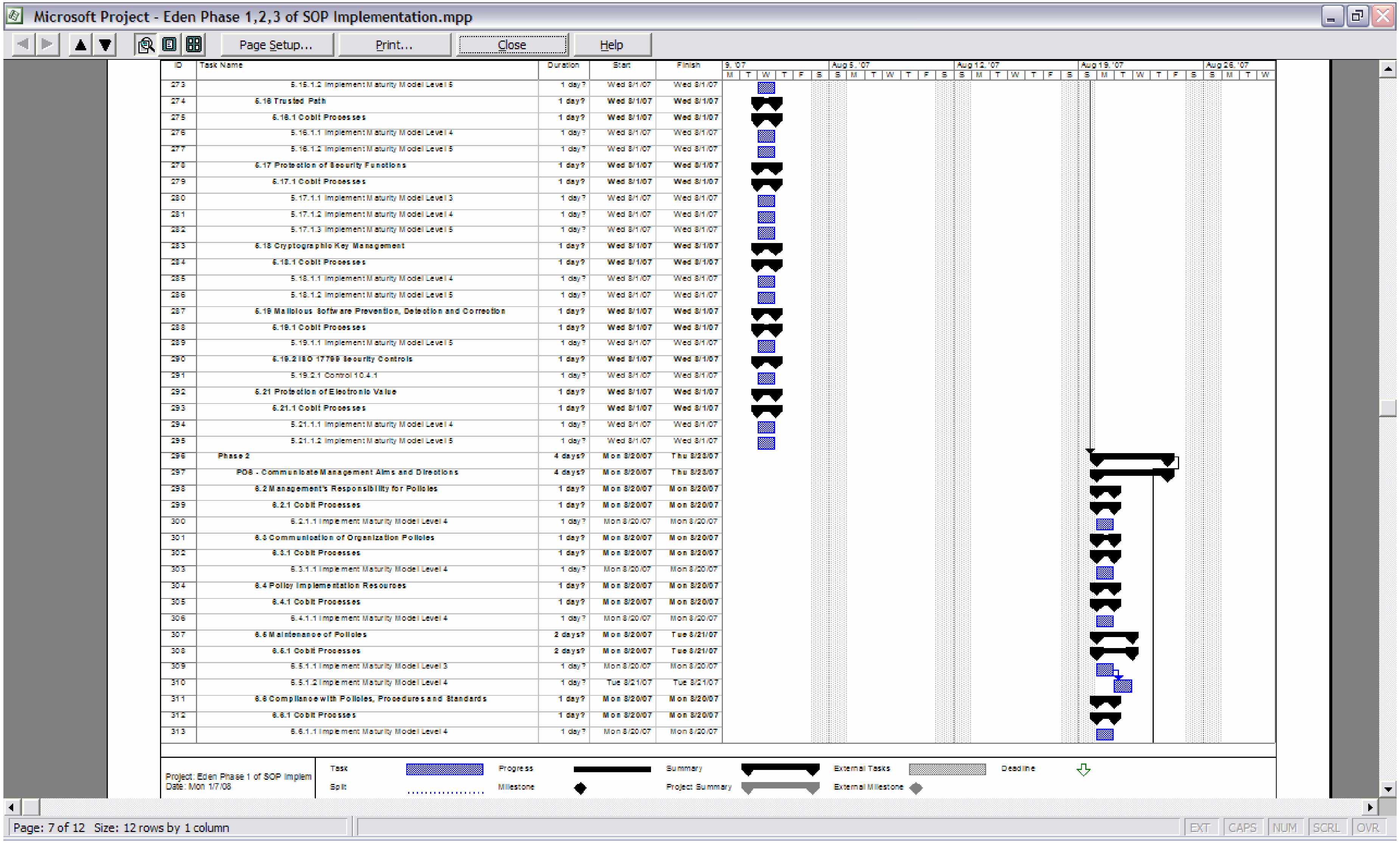


Microsoft Project - Eden Phase 1,2,3 of SOP Implementation.mpp
Page Setup...
Print...
Close
Help
9, '07
Aug 5, '07
Aug 12, '07
Aug 19, '07
Aug 26, '07
M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W
EXT
CAPS
NUM
SCRL
OVR

ID	Task Name	Duration	Start	Finish
232	5.7.2.6 Control 13.1.2	1 day?	Wed 8/1/07	Wed 8/1/07
233	5.7.2.7 Control 13.2.1	1 day?	Wed 8/1/07	Wed 8/1/07
234	5.7.2.8 Control 13.2.3	1 day?	Wed 8/1/07	Wed 8/1/07
235	**6.8 Data Classification**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
236	**6.8.1 Cobit Processes**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
237	5.8.1.1 Implement Maturity Model Level 3	1 day?	Wed 8/1/07	Wed 8/1/07
238	5.8.1.2 Implement Maturity Model Level 4	1 day?	Wed 8/1/07	Wed 8/1/07
239	5.8.1.3 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07
240	**6.8.2 ISO 17799 Security Controls**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
241	5.8.2.1 Control 7.2.1	1 day?	Wed 8/1/07	Wed 8/1/07
242	**6.9 Central Identification and Access Rights Management**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
243	**6.9.1 Cobit Processes**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
244	5.9.1.1 Implement Maturity Model Level 4	1 day?	Wed 8/1/07	Wed 8/1/07
245	5.9.1.2 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07
246	**6.10 Violation and Security Activity Reports**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
247	**6.10.1 Cobit Processes**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
248	5.10.1.1 Implement Maturity Model Level 3	1 day?	Wed 8/1/07	Wed 8/1/07
249	5.10.1.2 Implement Maturity Model Level 4	1 day?	Wed 8/1/07	Wed 8/1/07
250	5.10.1.3 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07
251	**6.10.2 ISO 17799 Security Controls**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
252	5.10.2.1 Control 15.2.1	1 day?	Wed 8/1/07	Wed 8/1/07
253	**6.11 Incident Handling**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
254	**6.11.1 Cobit Processes**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
255	5.11.1.1 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07
256	**6.12 Reaccreditation**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
257	**6.12.1 Cobit Processes**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
258	5.12.1.1 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07
259	**6.13 Counterparty Trust**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
260	**6.13.1 Cobit Processes**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
261	5.13.1.1 Implement Maturity Model Level 3	1 day?	Wed 8/1/07	Wed 8/1/07
262	5.13.1.2 Implement Maturity Model Level 4	1 day?	Wed 8/1/07	Wed 8/1/07
263	5.13.1.3 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07
264	**6.13.2 ISO 17799 Security Controls**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
265	5.13.2.1 Control 10.8.1	1 day?	Wed 8/1/07	Wed 8/1/07
266	**6.14 Transaction Authorization**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
267	**6.14.1 Cobit Processes**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
268	5.14.1.1 Implement Maturity Model Level 4	1 day?	Wed 8/1/07	Wed 8/1/07
269	5.14.1.2 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07
270	**6.15 Non-repudiation**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
271	**6.15.1 Cobit Processes**	**1 day?**	**Wed 8/1/07**	**Wed 8/1/07**
272	5.15.1.1 Implement Maturity Model Level 4	1 day?	Wed 8/1/07	Wed 8/1/07

Project: Eden Phase 1 of SOP Implem
Date: Mon 1/7/08

Page: 6 of 12 Size: 12 rows by 1 column

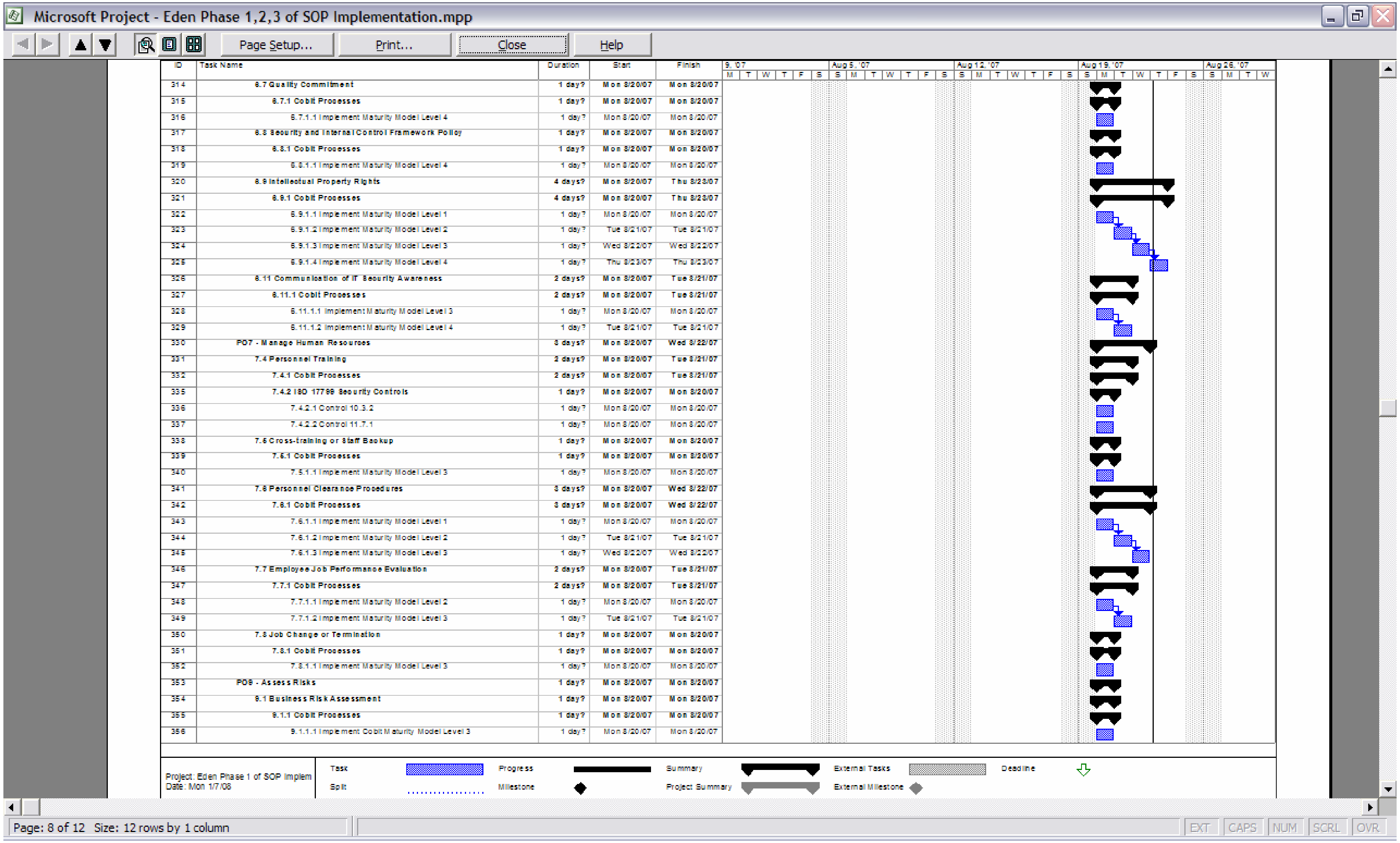


Microsoft Project - Eden Phase 1,2,3 of SOP Implementation.mpp
Page Setup...
Print...
Close
Help
9, '07
Aug 5, '07
Aug 12, '07
Aug 19, '07
Aug 26, '07
M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W
EXT
CAPS
NUM
SCRL
OVR

ID	Task Name	Duration	Start	Finish
273	5.15.1.2 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07
274	6.16 Trusted Path	1 day?	Wed 8/1/07	Wed 8/1/07
275	6.16.1 Cobit Processes	1 day?	Wed 8/1/07	Wed 8/1/07
276	5.16.1.1 Implement Maturity Model Level 4	1 day?	Wed 8/1/07	Wed 8/1/07
277	5.16.1.2 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07
278	6.17 Protection of Security Functions	1 day?	Wed 8/1/07	Wed 8/1/07
279	6.17.1 Cobit Processes	1 day?	Wed 8/1/07	Wed 8/1/07
280	5.17.1.1 Implement Maturity Model Level 3	1 day?	Wed 8/1/07	Wed 8/1/07
281	5.17.1.2 Implement Maturity Model Level 4	1 day?	Wed 8/1/07	Wed 8/1/07
282	5.17.1.3 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07
283	6.18 Cryptographic Key Management	1 day?	Wed 8/1/07	Wed 8/1/07
284	6.18.1 Cobit Processes	1 day?	Wed 8/1/07	Wed 8/1/07
285	5.18.1.1 Implement Maturity Model Level 4	1 day?	Wed 8/1/07	Wed 8/1/07
286	5.18.1.2 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07
287	6.19 Malicious Software Prevention, Detection and Correction	1 day?	Wed 8/1/07	Wed 8/1/07
288	6.19.1 Cobit Processes	1 day?	Wed 8/1/07	Wed 8/1/07
289	5.19.1.1 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07
290	6.19.2 ISO 17799 Security Controls	1 day?	Wed 8/1/07	Wed 8/1/07
291	5.19.2.1 Control 10.4.1	1 day?	Wed 8/1/07	Wed 8/1/07
292	6.21 Protection of Electronic Value	1 day?	Wed 8/1/07	Wed 8/1/07
293	6.21.1 Cobit Processes	1 day?	Wed 8/1/07	Wed 8/1/07
294	5.21.1.1 Implement Maturity Model Level 4	1 day?	Wed 8/1/07	Wed 8/1/07
295	5.21.1.2 Implement Maturity Model Level 5	1 day?	Wed 8/1/07	Wed 8/1/07
296	Phase 2	4 days?	Mon 8/20/07	Thu 8/23/07
297	PO6 - Communicate Management Aims and Directions	4 days?	Mon 8/20/07	Thu 8/23/07
298	6.2 Management's Responsibility for Policies	1 day?	Mon 8/20/07	Mon 8/20/07
299	6.2.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
300	6.2.1.1 Implement Maturity Model Level 4	1 day?	Mon 8/20/07	Mon 8/20/07
301	6.3 Communication of Organization Policies	1 day?	Mon 8/20/07	Mon 8/20/07
302	6.3.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
303	6.3.1.1 Implement Maturity Model Level 4	1 day?	Mon 8/20/07	Mon 8/20/07
304	6.4 Policy Implementation Resources	1 day?	Mon 8/20/07	Mon 8/20/07
305	6.4.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
306	6.4.1.1 Implement Maturity Model Level 4	1 day?	Mon 8/20/07	Mon 8/20/07
307	6.5 Maintenance of Policies	2 days?	Mon 8/20/07	Tue 8/21/07
308	6.5.1 Cobit Processes	2 days?	Mon 8/20/07	Tue 8/21/07
309	6.5.1.1 Implement Maturity Model Level 3	1 day?	Mon 8/20/07	Mon 8/20/07
310	6.5.1.2 Implement Maturity Model Level 4	1 day?	Tue 8/21/07	Tue 8/21/07
311	6.6 Compliance with Policies, Procedures and Standards	1 day?	Mon 8/20/07	Mon 8/20/07
312	6.6.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
313	6.6.1.1 Implement Maturity Model Level 4	1 day?	Mon 8/20/07	Mon 8/20/07

Project: Eden Phase 1 of SOP Implem
Date: Mon 1/7/08

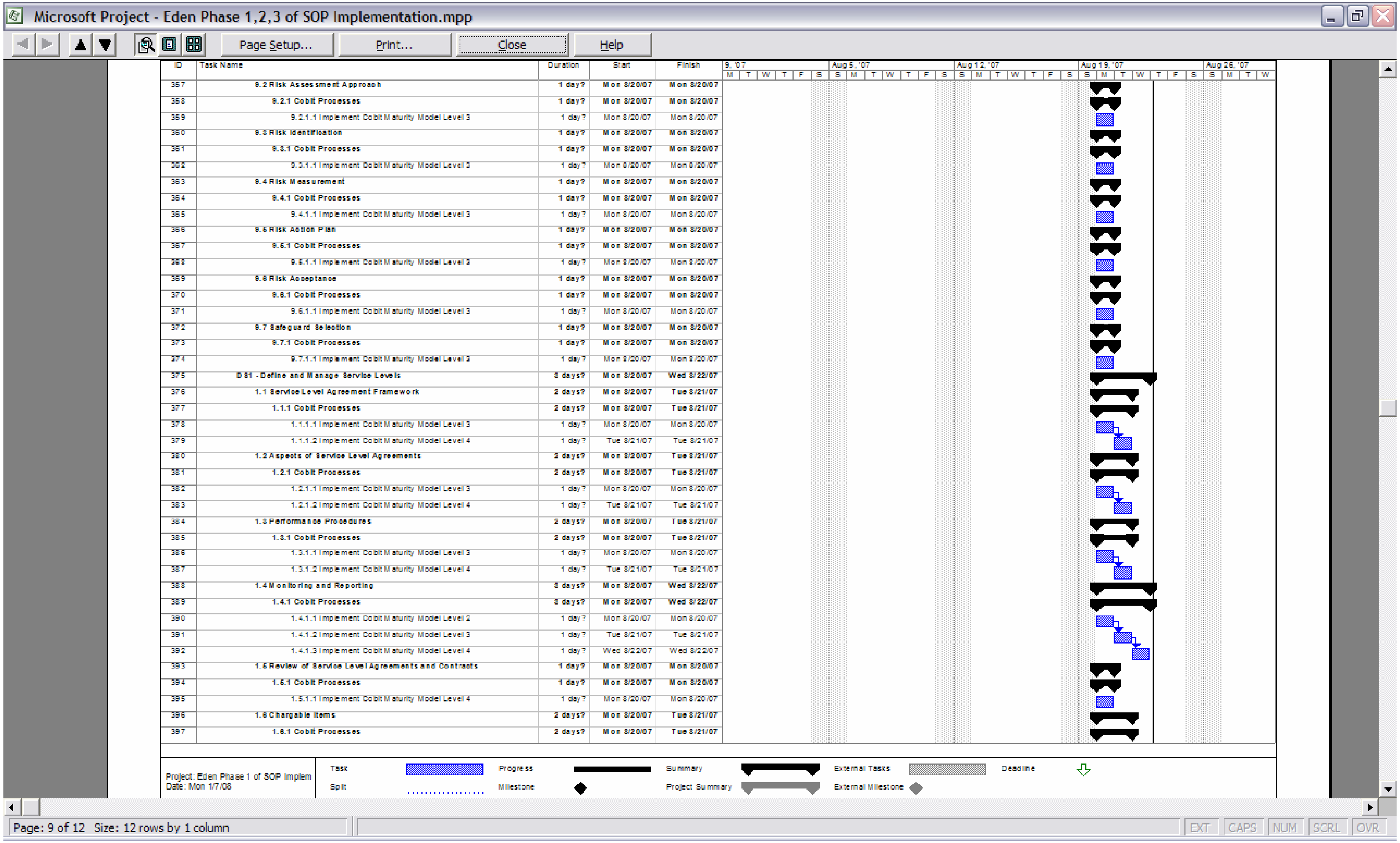
Page: 7 of 12 Size: 12 rows by 1 column


Microsoft Project - Eden Phase 1,2,3 of SOP Implementation.mpp
Page Setup...
Print...
Close
Help
9, '07
Aug 5, '07
Aug 12, '07
Aug 19, '07
Aug 26, '07
M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W

ID	Task Name	Duration	Start	Finish
314	6.7 Quality Commitment	1 day?	Mon 8/20/07	Mon 8/20/07
315	6.7.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
316	6.7.1.1 Implement Maturity Model Level 4	1 day?	Mon 8/20/07	Mon 8/20/07
317	6.8 Security and Internal Control Framework Policy	1 day?	Mon 8/20/07	Mon 8/20/07
318	6.8.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
319	6.8.1.1 Implement Maturity Model Level 4	1 day?	Mon 8/20/07	Mon 8/20/07
320	6.9 Intellectual Property Rights	4 days?	Mon 8/20/07	Thu 8/23/07
321	6.9.1 Cobit Processes	4 days?	Mon 8/20/07	Thu 8/23/07
322	6.9.1.1 Implement Maturity Model Level 1	1 day?	Mon 8/20/07	Mon 8/20/07
323	6.9.1.2 Implement Maturity Model Level 2	1 day?	Tue 8/21/07	Tue 8/21/07
324	6.9.1.3 Implement Maturity Model Level 3	1 day?	Wed 8/22/07	Wed 8/22/07
325	6.9.1.4 Implement Maturity Model Level 4	1 day?	Thu 8/23/07	Thu 8/23/07
326	6.11 Communication of IT Security Awareness	2 days?	Mon 8/20/07	Tue 8/21/07
327	6.11.1 Cobit Processes	2 days?	Mon 8/20/07	Tue 8/21/07
328	6.11.1.1 Implement Maturity Model Level 3	1 day?	Mon 8/20/07	Mon 8/20/07
329	6.11.1.2 Implement Maturity Model Level 4	1 day?	Tue 8/21/07	Tue 8/21/07
330	PO7 - Manage Human Resources	3 days?	Mon 8/20/07	Wed 8/22/07
331	7.4 Personnel Training	2 days?	Mon 8/20/07	Tue 8/21/07
332	7.4.1 Cobit Processes	2 days?	Mon 8/20/07	Tue 8/21/07
335	7.4.2 ISO 17799 Security Controls	1 day?	Mon 8/20/07	Mon 8/20/07
336	7.4.2.1 Control 10.3.2	1 day?	Mon 8/20/07	Mon 8/20/07
337	7.4.2.2 Control 11.7.1	1 day?	Mon 8/20/07	Mon 8/20/07
338	7.5 Cross-training or Staff Backup	1 day?	Mon 8/20/07	Mon 8/20/07
339	7.5.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
340	7.5.1.1 Implement Maturity Model Level 3	1 day?	Mon 8/20/07	Mon 8/20/07
341	7.6 Personnel Clearance Procedures	3 days?	Mon 8/20/07	Wed 8/22/07
342	7.6.1 Cobit Processes	3 days?	Mon 8/20/07	Wed 8/22/07
343	7.6.1.1 Implement Maturity Model Level 1	1 day?	Mon 8/20/07	Mon 8/20/07
344	7.6.1.2 Implement Maturity Model Level 2	1 day?	Tue 8/21/07	Tue 8/21/07
345	7.6.1.3 Implement Maturity Model Level 3	1 day?	Wed 8/22/07	Wed 8/22/07
346	7.7 Employee Job Performance Evaluation	2 days?	Mon 8/20/07	Tue 8/21/07
347	7.7.1 Cobit Processes	2 days?	Mon 8/20/07	Tue 8/21/07
348	7.7.1.1 Implement Maturity Model Level 2	1 day?	Mon 8/20/07	Mon 8/20/07
349	7.7.1.2 Implement Maturity Model Level 3	1 day?	Tue 8/21/07	Tue 8/21/07
350	7.8 Job Change or Termination	1 day?	Mon 8/20/07	Mon 8/20/07
351	7.8.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
352	7.8.1.1 Implement Maturity Model Level 3	1 day?	Mon 8/20/07	Mon 8/20/07
353	PO9 - Assess Risks	1 day?	Mon 8/20/07	Mon 8/20/07
354	9.1 Business Risk Assessment	1 day?	Mon 8/20/07	Mon 8/20/07
355	9.1.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
356	9.1.1.1 Implement Cobit Maturity Model Level 3	1 day?	Mon 8/20/07	Mon 8/20/07

Project: Eden Phase 1 of SOP Implem
Date: Mon 1/7/08

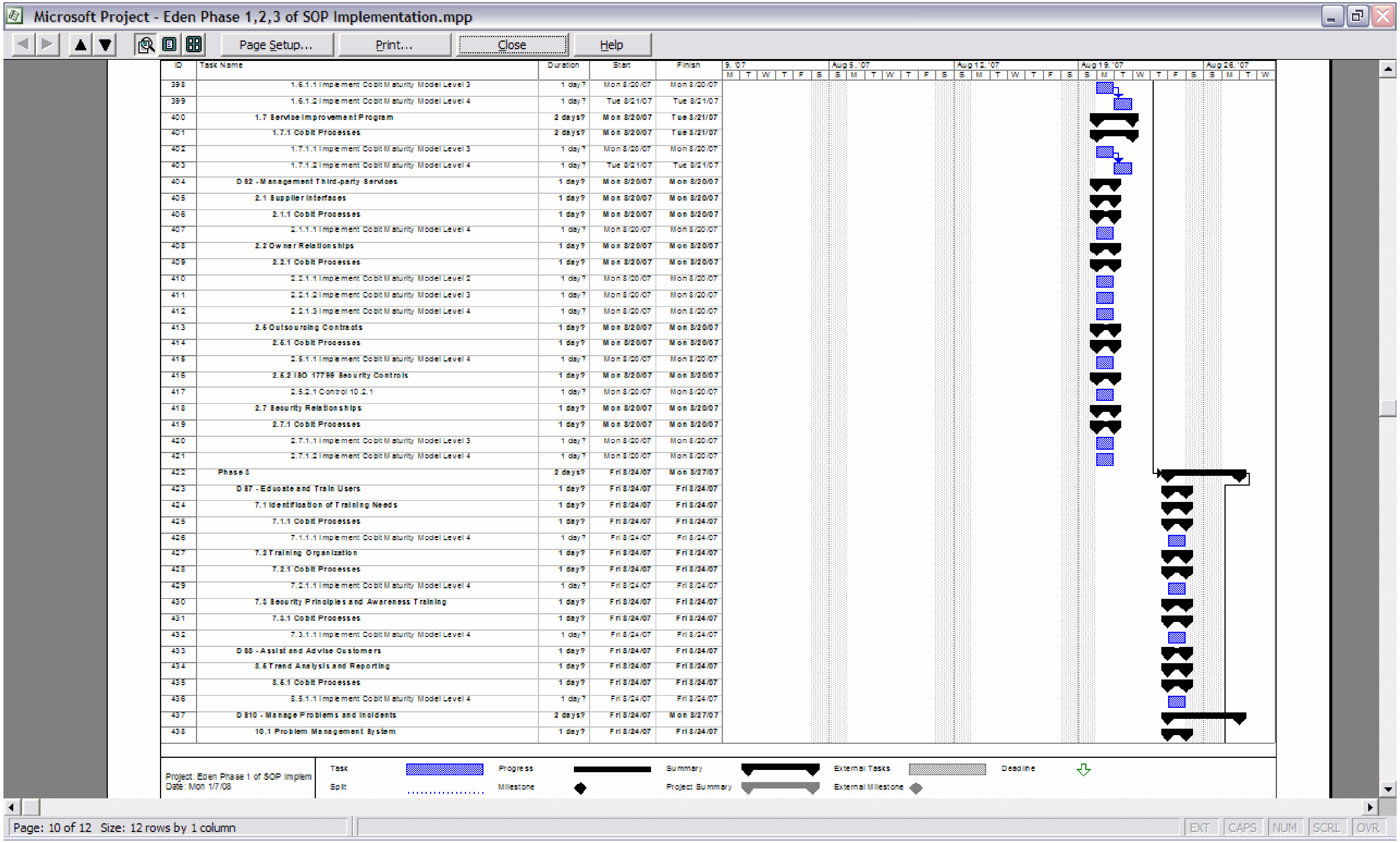
Page: 8 of 12 Size: 12 rows by 1 column


Microsoft Project - Eden Phase 1,2,3 of SOP Implementation.mpp
Page Setup...
Print...
Close
Help
9, '07
Aug 5, '07
Aug 12, '07
Aug 19, '07
Aug 26, '07
M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W

ID	Task Name	Duration	Start	Finish
357	9.2 Risk Assessment Approach	1 day?	Mon 8/20/07	Mon 8/20/07
358	9.2.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
359	9.2.1.1 Implement Cobit Maturity Model Level 3	1 day?	Mon 8/20/07	Mon 8/20/07
360	9.3 Risk Identification	1 day?	Mon 8/20/07	Mon 8/20/07
361	9.3.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
362	9.3.1.1 Implement Cobit Maturity Model Level 3	1 day?	Mon 8/20/07	Mon 8/20/07
363	9.4 Risk Measurement	1 day?	Mon 8/20/07	Mon 8/20/07
364	9.4.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
365	9.4.1.1 Implement Cobit Maturity Model Level 3	1 day?	Mon 8/20/07	Mon 8/20/07
366	9.5 Risk Action Plan	1 day?	Mon 8/20/07	Mon 8/20/07
367	9.5.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
368	9.5.1.1 Implement Cobit Maturity Model Level 3	1 day?	Mon 8/20/07	Mon 8/20/07
369	9.6 Risk Acceptance	1 day?	Mon 8/20/07	Mon 8/20/07
370	9.6.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
371	9.6.1.1 Implement Cobit Maturity Model Level 3	1 day?	Mon 8/20/07	Mon 8/20/07
372	9.7 Safeguard Selection	1 day?	Mon 8/20/07	Mon 8/20/07
373	9.7.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
374	9.7.1.1 Implement Cobit Maturity Model Level 3	1 day?	Mon 8/20/07	Mon 8/20/07
375	DS1 - Define and Manage Service Levels	3 days?	Mon 8/20/07	Wed 8/22/07
376	1.1 Service Level Agreement Framework	2 days?	Mon 8/20/07	Tue 8/21/07
377	1.1.1 Cobit Processes	2 days?	Mon 8/20/07	Tue 8/21/07
378	1.1.1.1 Implement Cobit Maturity Model Level 3	1 day?	Mon 8/20/07	Mon 8/20/07
379	1.1.1.2 Implement Cobit Maturity Model Level 4	1 day?	Tue 8/21/07	Tue 8/21/07
380	1.2 Aspects of Service Level Agreements	2 days?	Mon 8/20/07	Tue 8/21/07
381	1.2.1 Cobit Processes	2 days?	Mon 8/20/07	Tue 8/21/07
382	1.2.1.1 Implement Cobit Maturity Model Level 3	1 day?	Mon 8/20/07	Mon 8/20/07
383	1.2.1.2 Implement Cobit Maturity Model Level 4	1 day?	Tue 8/21/07	Tue 8/21/07
384	1.3 Performance Procedures	2 days?	Mon 8/20/07	Tue 8/21/07
385	1.3.1 Cobit Processes	2 days?	Mon 8/20/07	Tue 8/21/07
386	1.3.1.1 Implement Cobit Maturity Model Level 3	1 day?	Mon 8/20/07	Mon 8/20/07
387	1.3.1.2 Implement Cobit Maturity Model Level 4	1 day?	Tue 8/21/07	Tue 8/21/07
388	1.4 Monitoring and Reporting	3 days?	Mon 8/20/07	Wed 8/22/07
389	1.4.1 Cobit Processes	3 days?	Mon 8/20/07	Wed 8/22/07
390	1.4.1.1 Implement Cobit Maturity Model Level 2	1 day?	Mon 8/20/07	Mon 8/20/07
391	1.4.1.2 Implement Cobit Maturity Model Level 3	1 day?	Tue 8/21/07	Tue 8/21/07
392	1.4.1.3 Implement Cobit Maturity Model Level 4	1 day?	Wed 8/22/07	Wed 8/22/07
393	1.5 Review of Service Level Agreements and Contracts	1 day?	Mon 8/20/07	Mon 8/20/07
394	1.5.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
395	1.5.1.1 Implement Cobit Maturity Model Level 4	1 day?	Mon 8/20/07	Mon 8/20/07
396	1.6 Chargable Items	2 days?	Mon 8/20/07	Tue 8/21/07
397	1.6.1 Cobit Processes	2 days?	Mon 8/20/07	Tue 8/21/07

Project: Eden Phase 1 of SOP Implem
Date: Mon 1/7/08

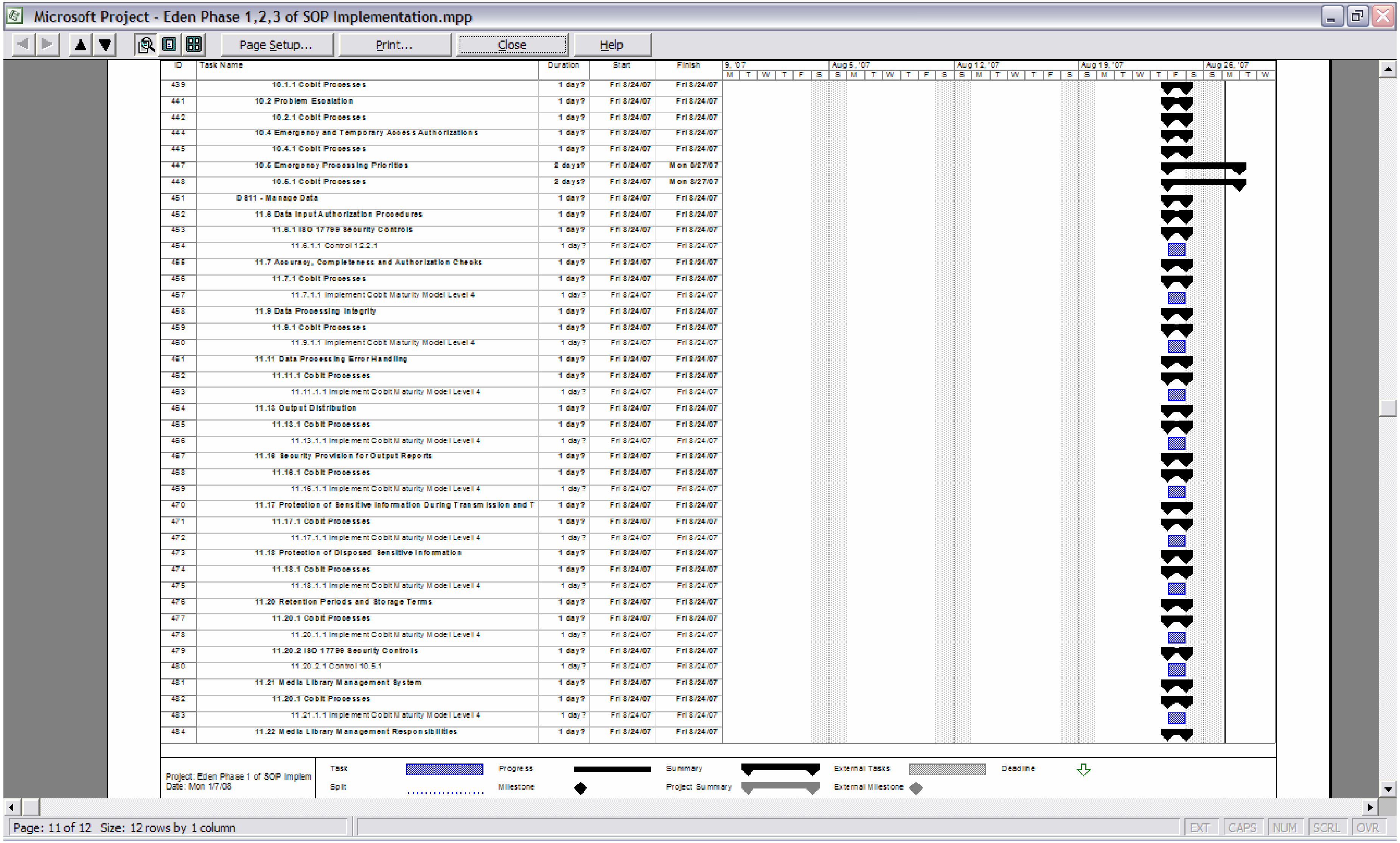
Page: 9 of 12 Size: 12 rows by 1 column


Microsoft Project - Eden Phase 1,2,3 of SOP Implementation.mpp
Page Setup...
Print...
Close
Help
9, '07
Aug 5, '07
Aug 12, '07
Aug 19, '07
Aug 26, '07
M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W

ID	Task Name	Duration	Start	Finish
398	1.6.1.1 Implement Cobit Maturity Model Level 3	1 day?	Mon 8/20/07	Mon 8/20/07
399	1.6.1.2 Implement Cobit Maturity Model Level 4	1 day?	Tue 8/21/07	Tue 8/21/07
400	1.7 Service Improvement Program	2 days?	Mon 8/20/07	Tue 8/21/07
401	1.7.1 Cobit Processes	2 days?	Mon 8/20/07	Tue 8/21/07
402	1.7.1.1 Implement Cobit Maturity Model Level 3	1 day?	Mon 8/20/07	Mon 8/20/07
403	1.7.1.2 Implement Cobit Maturity Model Level 4	1 day?	Tue 8/21/07	Tue 8/21/07
404	D S2 - Management Third-party Services	1 day?	Mon 8/20/07	Mon 8/20/07
405	2.1 Supplier Interfaces	1 day?	Mon 8/20/07	Mon 8/20/07
406	2.1.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
407	2.1.1.1 Implement Cobit Maturity Model Level 4	1 day?	Mon 8/20/07	Mon 8/20/07
408	2.2 Owner Relationships	1 day?	Mon 8/20/07	Mon 8/20/07
409	2.2.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
410	2.2.1.1 Implement Cobit Maturity Model Level 2	1 day?	Mon 8/20/07	Mon 8/20/07
411	2.2.1.2 Implement Cobit Maturity Model Level 3	1 day?	Mon 8/20/07	Mon 8/20/07
412	2.2.1.3 Implement Cobit Maturity Model Level 4	1 day?	Mon 8/20/07	Mon 8/20/07
413	2.5 Outsourcing Contracts	1 day?	Mon 8/20/07	Mon 8/20/07
414	2.5.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
415	2.5.1.1 Implement Cobit Maturity Model Level 4	1 day?	Mon 8/20/07	Mon 8/20/07
416	2.5.2 ISO 17799 Security Controls	1 day?	Mon 8/20/07	Mon 8/20/07
417	2.5.2.1 Control 10.2.1	1 day?	Mon 8/20/07	Mon 8/20/07
418	2.7 Security Relationships	1 day?	Mon 8/20/07	Mon 8/20/07
419	2.7.1 Cobit Processes	1 day?	Mon 8/20/07	Mon 8/20/07
420	2.7.1.1 Implement Cobit Maturity Model Level 3	1 day?	Mon 8/20/07	Mon 8/20/07
421	2.7.1.2 Implement Cobit Maturity Model Level 4	1 day?	Mon 8/20/07	Mon 8/20/07
422	Phase 3	2 days?	Fri 8/24/07	Mon 8/27/07
423	D S7 - Educate and Train Users	1 day?	Fri 8/24/07	Fri 8/24/07
424	7.1 Identification of Training Needs	1 day?	Fri 8/24/07	Fri 8/24/07
425	7.1.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
426	7.1.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
427	7.2 Training Organization	1 day?	Fri 8/24/07	Fri 8/24/07
428	7.2.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
429	7.2.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
430	7.3 Security Principles and Awareness Training	1 day?	Fri 8/24/07	Fri 8/24/07
431	7.3.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
432	7.3.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
433	D S8 - Assist and Advise Customers	1 day?	Fri 8/24/07	Fri 8/24/07
434	8.5 Trend Analysis and Reporting	1 day?	Fri 8/24/07	Fri 8/24/07
435	8.5.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
436	8.5.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
437	D S10 - Manage Problems and Incidents	2 days?	Fri 8/24/07	Mon 8/27/07
438	10.1 Problem Management System	1 day?	Fri 8/24/07	Fri 8/24/07

Project: Eden Phase 1 of SOP Implem
Date: Mon 1/7/08

Page: 10 of 12 Size: 12 rows by 1 column

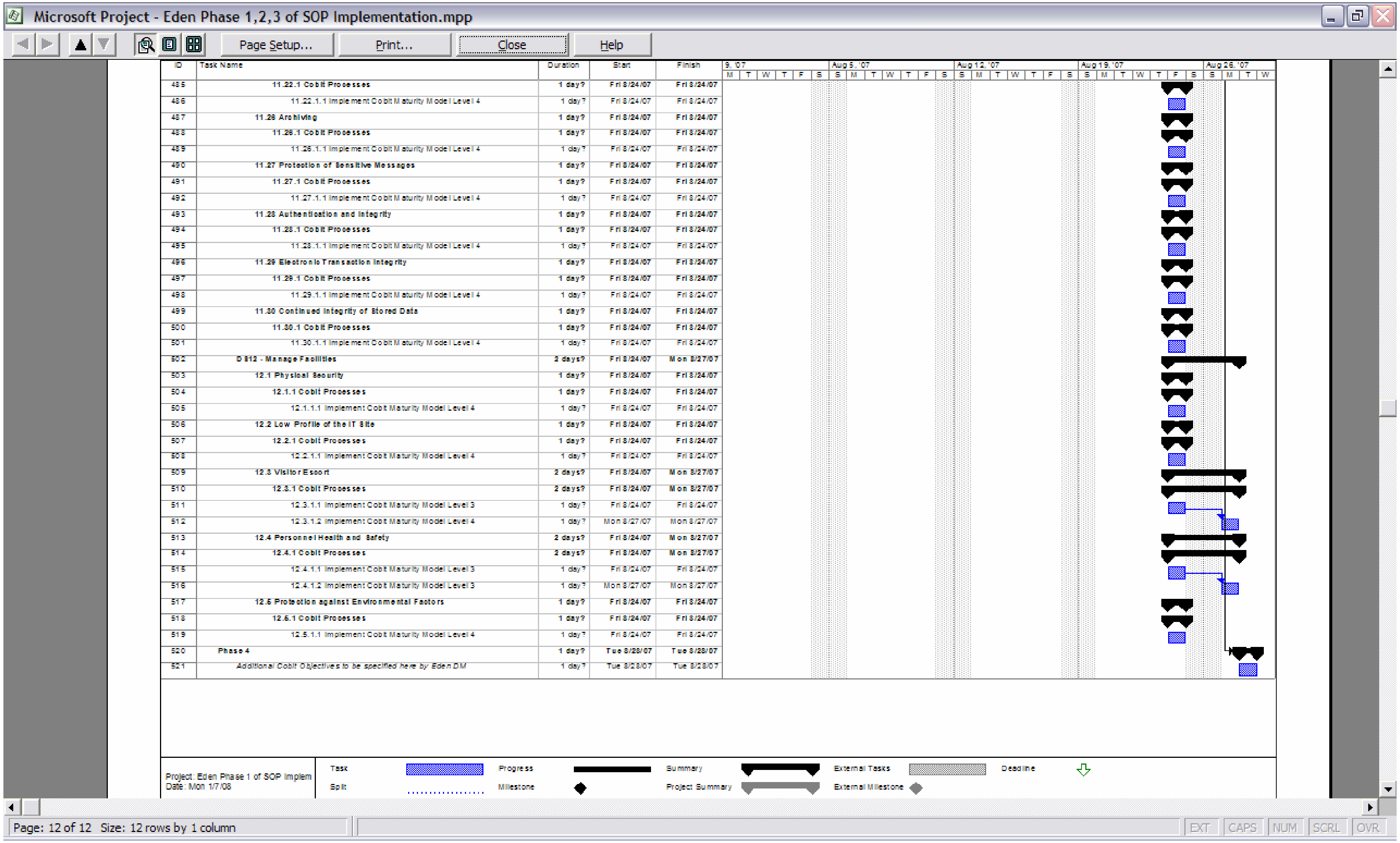

Microsoft Project - Eden Phase 1,2,3 of SOP Implementation.mpp
Page Setup...
Print...
Close
Help
9, '07
Aug 5, '07
Aug 12, '07
Aug 19, '07
Aug 26, '07
M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W
EXT
CAPS
NUM
SCRL
OVR

ID	Task Name	Duration	Start	Finish
439	10.1.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
441	10.2 Problem Escalation	1 day?	Fri 8/24/07	Fri 8/24/07
442	10.2.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
444	10.4 Emergency and Temporary Access Authorizations	1 day?	Fri 8/24/07	Fri 8/24/07
445	10.4.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
447	10.5 Emergency Processing Priorities	2 days?	Fri 8/24/07	Mon 8/27/07
448	10.5.1 Cobit Processes	2 days?	Fri 8/24/07	Mon 8/27/07
451	D S11 - Manage Data	1 day?	Fri 8/24/07	Fri 8/24/07
452	11.6 Data Input Authorization Procedures	1 day?	Fri 8/24/07	Fri 8/24/07
453	11.6.1 ISO 17799 Security Controls	1 day?	Fri 8/24/07	Fri 8/24/07
454	11.6.1.1 Control 12.2.1	1 day?	Fri 8/24/07	Fri 8/24/07
455	11.7 Accuracy, Completeness and Authorization Checks	1 day?	Fri 8/24/07	Fri 8/24/07
456	11.7.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
457	11.7.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
458	11.9 Data Processing Integrity	1 day?	Fri 8/24/07	Fri 8/24/07
459	11.9.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
460	11.9.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
461	11.11 Data Processing Error Handling	1 day?	Fri 8/24/07	Fri 8/24/07
462	11.11.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
463	11.11.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
464	11.13 Output Distribution	1 day?	Fri 8/24/07	Fri 8/24/07
465	11.13.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
466	11.13.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
467	11.16 Security Provision for Output Reports	1 day?	Fri 8/24/07	Fri 8/24/07
468	11.16.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
469	11.16.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
470	11.17 Protection of Sensitive Information During Transmission and T	1 day?	Fri 8/24/07	Fri 8/24/07
471	11.17.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
472	11.17.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
473	11.18 Protection of Disposed Sensitive Information	1 day?	Fri 8/24/07	Fri 8/24/07
474	11.18.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
475	11.18.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
476	11.20 Retention Periods and Storage Terms	1 day?	Fri 8/24/07	Fri 8/24/07
477	11.20.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
478	11.20.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
479	11.20.2 ISO 17799 Security Controls	1 day?	Fri 8/24/07	Fri 8/24/07
480	11.20.2.1 Control 10.5.1	1 day?	Fri 8/24/07	Fri 8/24/07
481	11.21 Media Library Management System	1 day?	Fri 8/24/07	Fri 8/24/07
482	11.20.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
483	11.21.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
484	11.22 Media Library Management Responsibilities	1 day?	Fri 8/24/07	Fri 8/24/07

Project: Eden Phase 1 of SOP Implem
Date: Mon 1/7/08

Task	▨	Progress	▬	Summary	▬	External Tasks	▨	Deadline	⇩
Split	⋯	Milestone	◆	Project Summary	▬	External Milestone	◆		

Page: 11 of 12 Size: 12 rows by 1 column



ID	Task Name	Duration	Start	Finish
485	11.22.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
486	11.22.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
487	11.26 Archiving	1 day?	Fri 8/24/07	Fri 8/24/07
488	11.26.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
489	11.26.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
490	11.27 Protection of Sensitive Messages	1 day?	Fri 8/24/07	Fri 8/24/07
491	11.27.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
492	11.27.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
493	11.28 Authentication and Integrity	1 day?	Fri 8/24/07	Fri 8/24/07
494	11.28.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
495	11.28.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
496	11.29 Electronic Transaction Integrity	1 day?	Fri 8/24/07	Fri 8/24/07
497	11.29.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
498	11.29.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
499	11.30 Continued Integrity of Stored Data	1 day?	Fri 8/24/07	Fri 8/24/07
500	11.30.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
501	11.30.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
502	D S12 - Manage Facilities	2 days?	Fri 8/24/07	Mon 8/27/07
503	12.1 Physical Security	1 day?	Fri 8/24/07	Fri 8/24/07
504	12.1.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
505	12.1.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
506	12.2 Low Profile of the IT Site	1 day?	Fri 8/24/07	Fri 8/24/07
507	12.2.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
508	12.2.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
509	12.3 Visitor Escort	2 days?	Fri 8/24/07	Mon 8/27/07
510	12.3.1 Cobit Processes	2 days?	Fri 8/24/07	Mon 8/27/07
511	12.3.1.1 Implement Cobit Maturity Model Level 3	1 day?	Fri 8/24/07	Fri 8/24/07
512	12.3.1.2 Implement Cobit Maturity Model Level 4	1 day?	Mon 8/27/07	Mon 8/27/07
513	12.4 Personnel Health and Safety	2 days?	Fri 8/24/07	Mon 8/27/07
514	12.4.1 Cobit Processes	2 days?	Fri 8/24/07	Mon 8/27/07
515	12.4.1.1 Implement Cobit Maturity Model Level 3	1 day?	Fri 8/24/07	Fri 8/24/07
516	12.4.1.2 Implement Cobit Maturity Model Level 3	1 day?	Mon 8/27/07	Mon 8/27/07
517	12.5 Protection against Environmental Factors	1 day?	Fri 8/24/07	Fri 8/24/07
518	12.5.1 Cobit Processes	1 day?	Fri 8/24/07	Fri 8/24/07
519	12.5.1.1 Implement Cobit Maturity Model Level 4	1 day?	Fri 8/24/07	Fri 8/24/07
520	Phase 4	1 day?	Tue 8/28/07	Tue 8/28/07
521	*Additional Cobit Objectives to be specified here by Eden DM*	1 day?	Tue 8/28/07	Tue 8/28/07

Project: Eden Phase 1 of SOP Implem
Date: Mon 1/7/08

Page: 12 of 12 Size: 12 rows by 1 column

Appendix H

Papers Presented and Published

H.1 Paper 1

In November 2006, at the conference of the "Suid-Afrikaanse Akademie vir Wetenskap en Kuns" held in Potchefstroom, South Africa, a paper and poster were presented, titled: "IT Korporatiewe Bestuur in Plaaslike Munisipaliteite: Op pad na 'n Normpraktyk."

Abstract

Vandag speel tegnologie 'n veel groter rol in besighede en organisasies as ooit tevore. Informasie word as die "lewensbloed" van 'n organisasie beskou – die heel belangrikste bate. Met die groot verskeidenheid moontlikhede wat inligtingstegnologie (IT) vandag vir besighede en organisasies bied en die aantal besigheidsprosesse wat deur IT gedryf word, is dit 'n alombekende feit dat IT 'n organisasie kan maak of breek, afhangende van hoe dit bestuur word. Tans is daar baie min, indien enige, wetgewing of raamwerke wat as voorskrif dien vir die ontwikkeling en bestuur van IT in plaaslike munisipaliteite. Daar is gevolglik talle probleme wat tans ondervind word. Die doel van hierdie navorsing is om as resultaat, 'n omvattende, praktiese raamwerk voor te stel wat op internasionale normpraktyke gebaseer is, aangepas is vir die munisipale sektor en in kwantitatiewe terme gemeet kan word om die probleme wat tans ondervind word, aan te spreek.

Publication and Reference

This paper was published as a short paper in the following journal:
"Die Suid-Afrikaanse Tydskrif vir Natuurwetenskap en Tegnologie." Published by the "Suid-Afrikaanse Akademie vir Wetenskap en Kuns", Year 26, No.2, June 2007. Page 159.

H.2 Project Presentation – LogICT Western Cape

In November 2006, at the Local Government ICT Forum (LogICT) of the Western Cape, held in Wilderness, George, a paper was presented.

H.3 Project Presentation – COGITRIS II

In August 2007, at the COGITRIS II conference, held in Port Elizabeth, South Africa, a paper was presented.

H.4 Project Presentation – SAICSIT 2007

In September 2007, at the SAICSIT 2007 conference, held at the Fish River Sun, South Africa, a paper and poster were presented, titled: "Corporate and IT Governance in Local Municipalities: Towards a Best Practice."

Abstract

South African Municipalities are required, by Law, to perform strategic planning through means of compiling an Integrated Development Plan (IDP) document in order to meet specific, government-defined goals. Information Technology (IT) holds many advantages for the implementation of these goals if the IT systems and the business processes can be aligned with the IDP-goals. It is therefore necessary to govern the IT infrastructure, by means of an IT management plan, to ensure that the IT goals complement the long-range IDP strategy. This paper discusses the background, criteria and content of such a plan which is based on COBIT and ISO 17799 international Best Practices.

H.5 Paper 2 – IST Africa 2008

A paper was submitted to the IST Africa 2008 Conference and Exhibition in Namibia.