A Framework for IT Governance in Small Businesses

by

Herman Koornhof
A Framework for IT Governance in Small Businesses

by

Herman Koornhof

Treatise

Submitted for the partial fulfilment of the requirements for the degree

Magister Technologiae

in

Business Information Systems

in the

Faculty of Engineering, the Built Environment and Information Technology

of the

Nelson Mandela Metropolitan University

Supervisor: Prof. Rossouw von Solms

January 2009
Declaration

I, Herman Koornhof, hereby declare that:

- The work in this treatise is my own work.

- All sources used or referred to have been documented and recognised.

- This treatise has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognised educational institution.

______________________________
Herman Koornhof
Acknowledgements

I would like to express my gratitude to the following people:

- My love, Jenny, for your love and understanding during the past year. Without your encouragement and inspiration this work would not have been possible.

- My family and friends for your interest and support.

- My supervisor, Prof. Rossouw von Solms, for your guidance and advice, and your detailed and constructive comments.

- To Him who is able to do immeasurably more than all we ask or imagine, according to his power that is at work within us.
Table of Contents

Declaration ........................................................................................................... iii
Acknowledgements .............................................................................................. iv
Table of Contents .................................................................................................. v
List of Figures and Tables .................................................................................. ix

Chapter 1 – Introduction ...................................................................................... 1
  1.1 Background ................................................................................................. 1
  1.2 Area of study ............................................................................................... 3
  1.3 Problem statement ...................................................................................... 5
  1.4 Objectives .................................................................................................... 5
  1.5 Methodology ................................................................................................ 6
  1.6 Layout and conclusion ................................................................................ 6

Chapter 2 – Small Businesses ........................................................................... 10
  2.1 Introduction ............................................................................................... 11
  2.2 What is a small business? ........................................................................ 11
    2.2.1 Classification in various countries .............................................. 12
    2.2.2 Classification by various researchers ......................................... 15
    2.2.3 The term “small business” in different contexts ....................... 16
  2.3 The importance of small businesses ........................................................ 17
  2.4 Forms of ownership of small businesses ................................................. 18
    2.4.1 Sole proprietors ............................................................................ 18
    2.4.2 Partnerships ................................................................................. 19
    2.4.3 Independent legal entities ........................................................... 20
  2.5 Management in small businesses ............................................................ 25
  2.6 Problems facing small businesses ............................................................ 26
  2.7 Conclusion ................................................................................................. 27

Chapter 3 – Corporate Governance ................................................................... 29
  3.1 Introduction ............................................................................................... 30
5.4 Characteristics of IT governance in small businesses

5.4.1 No boards of directors
5.4.2 Limited management structures
5.4.3 Small or non-existent IT departments
5.4.4 Lack of resources
5.4.5 Less complex frameworks
5.4.6 Focus on information security
5.4.7 Low-cost systems

5.5 Conclusion

Chapter 6 – The ITGovSB Framework

6.1 Introduction
6.2 Why a framework for small businesses is needed
6.3 ITGovSB and what it involves
6.4 The ITGovSB framework
6.5 Evaluating ITGovSB against the characteristics of IT governance in small businesses

6.5.1 No boards of directors
6.5.2 Limited management structures
6.5.3 Small or non-existent IT departments
6.5.4 Lack of resources
6.5.5 Less complex frameworks
6.5.6 Focus on information security
6.5.7 Low-cost systems

6.6 Conclusion

Chapter 7 – Implementing ITGovSB: A Case Study

7.1 Introduction
7.2 The small business
7.3 The situation before implementing ITGovSB
7.4 The implementation process

7.4.1 Stage one
7.4.2 Stage two
List of Figures and Tables

Figure 1.1 Layout of chapters .......................................................... 7

Figure 2.1 Schedule referred to in the National Small Business Amendment Bill of 2003................................. 13

Figure 2.2 Classification of business by size according to the SBA...................... 14

Figure 2.3 The term “small business” in different contexts.......................... 16

Figure 2.4 Relative position of United States proprietorships, partnerships and corporations........................................... 24

Figure 2.5 Comparison of proprietorships, partnerships and corporations in selected industries .................................. 24

Figure 2.6 Management models....................................................... 26

Figure 4.1 IT governance and IT management....................................... 50

Figure 4.2 Basic CobiT principle...................................................... 59

Figure 4.3 The CobiT framework.................................................... 62

Table 5.1 Controls that SMEs should have in place for securing information assets ......................................................... 77

Figure 6.1 The ITGovSB domains and processes .................................. 90

Table 7.1 Findings and recommendations made by the IT auditors .......... 121
Chapter 1

Introduction

1.1 Background

Due to corporate governance malpractices such as the scandals of Enron and WorldCom, and the dramatic decline of stock markets at the beginning of the new century, the subject of corporate governance has received much attention recently (Letza, Kirkbride, Sun & Smallman, 2008, p. 17). Corporate governance principles were developed because investors were worried about the excessive concentration of power in the hands of management (King Committee, 2002, p. 9).

Corporate governance is the system by which companies are directed and controlled and is the responsibility of the board of directors (Cadbury Committee, 1992, p. 15). While management can be seen as running an organisation, governance is about making sure that the organisation is run properly (Naidoo, 2002, p. 1).

Companies are governed within the framework of the laws and regulations of the country in which they operate. Communities and countries differ in their culture, regulation, law and generally the way business is done (King Committee, 2002, p. 14). The King Committee was formed in 1992 to consider corporate governance in the context of South Africa. Corporate governance in South Africa was institutionalised by the publication of the first King Report on Corporate Governance (King Report) in 1994. The King Report on Corporate Governance 2002 (King II Report) is the second report of the King Committee. The Sarbanes-Oxley Act of 2002 was passed to re-establish confidence in corporate governance in the United States. Since initiating the development of corporate governance in the United Kingdom in 1992, the
Cadbury Report has been updated and combined with various other reports to form the Combined Code.

IT governance is an integral part of enterprise governance (IT Governance Institute, 2003, p. 10). The need to integrate IT governance with overall governance is similar to the need for IT to be an integral part of the enterprise rather than something practised in remote corners (IT Governance Institute, 2003, p. 6).

The use of IT has the potential to be the major driver of economic wealth in the 21st century. While IT is already critical to enterprise success, provides opportunities to obtain a competitive advantage and offers a means for increasing productivity, it will do all this even more so in the future (IT Governance Institute, 2003, p. 14).

Successful deployment of IT governance creates numerous benefits for business and IT. IT governance consists of the leadership and organisational structures and processes that ensure that the organisation’s IT sustains and extends the organisation’s strategies and objectives (IT Governance Institute, 2003, p. 10). In general, IT governance has five main focus areas. Two of these are outcomes: value delivery and risk management. The other three are drivers: strategic alignment, resource management (which overlays them all) and performance measurement (IT Governance Institute, 2003, p. 19).

Organisations can approach IT governance on an ad hoc basis and create their own frameworks based on the best practice experience found within the organisation, or they can adopt standards that have been developed and refined through the combined experience of hundreds of organisations and people. By adopting a standard IT governance framework, enterprises realise a number of benefits (Spafford, 2003).

A number of standard IT governance frameworks exist today. The Control Objectives for Information and Related Technology (CobiT) is focused on what
is required to achieve adequate management and control of IT, and is positioned at a high level. The CobiT framework was created with the main characteristics of being business-focused, process-oriented, controls-based and measurement-driven (IT Governance Institute, 2007, p. 10). The ISO/IEC 27000-series is comprised of information security standards. ISO/IEC 27002 provides best practice recommendations on information security management, while ISO/IEC 27001 is the certification standard against which organisations may be certified (ISO 27000 Directory, 2008). The IT Infrastructure Library (ITIL) is a set of best practices for IT service management, and aims to provide best practice definitions and criteria for operations management within service support and service delivery (APM Group, 2008).

In this treatise, IT governance and IT governance frameworks will be studied in the context of small businesses.

1.2 Area of study

The issue of what constitutes a small or medium enterprise is a matter of concern in the small and medium-sized enterprise (SME) literature (Abor & Adjasi, 2007, p. 112). The classification of firms by size varies among countries, researchers and other bodies. Some use the number of employees, some use capital assets, while others use turnover level. Some even define SMEs in terms of their legal status and method of production. Most researchers, however, use the number of employees to define businesses by size.

The size of a small business in different definitions varies quite dramatically. For the purposes of this study, which uses the South African National Small Business Act of 1996 (South Africa, 1996) as a guide, a small business means one with 50 employees or less.
Corporate governance has traditionally been associated with larger organisations. This is mainly due to the separation between ownership and control of the firm. Also, the question of accountability by small businesses to the public does not apply since they do not depend on public funds (Abor & Biekpe, 2007, p. 290).

In spite of these arguments, there is a global concern for the application of corporate governance to small and medium-sized enterprises. It is often argued that similar guidelines that apply to listed companies should also be applicable to such enterprises. Small businesses can benefit considerably from applying corporate governance principles and the existence of a board of directors. Corporate governance can establish better management practices and performance, and provide easier access to funding. Non-executive directors can assist small businesses in better decision-making and in attracting resources.

Similar to corporate governance, IT governance is often perceived as something only relevant to large organisations. This is, however, not the case. IT governance is a key element of every organisation, irrespective of its size (De Graaf, 2008). IT governance is about applying IT in such a way that it creates value for the business, while balancing the risk versus return. Small businesses also want to create value by applying IT. This, together with the fact that corporate governance, of which IT governance is a subset, applies to small businesses, makes IT governance applicable to small businesses as well (De Graaf, 2008).

IT functions in small businesses differ from those in larger organisations. The IT functions in small businesses tend to have a more centralised structure with the CEO or business owner. Small businesses also, generally, have difficulty in attracting and retaining skilled IT staff, and, therefore, have smaller or no IT departments and a lack of IT specialists. This is mostly due to the lack of resources that can be associated with small businesses (Yang & Jing, 2008, p. 326).
Due to the significant differences between IT in small businesses and large organisations, IT governance and the implementation thereof also differs quite considerably between these organisations.

1.3 Problem statement

There are many frameworks available to assist organisations in implementing IT governance. Most of these frameworks are, however, intended for large organisations with access to many resources.

Existing frameworks like CobiT can be overwhelming for small businesses to implement. They are too complex and costly and small businesses may consider the process intimidating and unachievable (Upfold & Sewry, 2005, p. 5)

Existing frameworks require many resources to implement. Small businesses, however, generally suffer from a lack of resources. A small business with limited staff resources is going to need a consultant to help implement IT governance controls (Armstrong, 2008). Organisations implementing IT governance frameworks spend a lot of money on implementing and hiring consultants (IT Business Edge, 2006). Due to financial constraints small businesses may not be able to afford hiring consultants to implement IT governance.

An alternative IT governance framework aimed specifically at small businesses is necessary to solve the problem. Such a framework must be less complex and extensive than existing frameworks and require fewer resources to implement.

1.4 Objectives

The primary objective of this treatise is to develop a framework that small businesses can use to implement IT governance. This framework for IT
Governance in Small Businesses, called ITGovSB, will be based primarily on the CobiT framework and the ISO/IEC 27002 information security controls.

In order to achieve the primary objective, it is necessary to understand the differences between IT governance in small businesses and larger organisations. Consequently, one of the secondary objectives of the paper is to derive characteristics that define IT governance in small businesses.

Another secondary objective is to implement the ITGovSB framework at a small business to evaluate its effectiveness.

1.5 Methodology

The first part of the treatise will consist of a detailed literature study. Literature regarding small businesses, corporate governance and IT governance will be studied and analysed. The aim of the literature study is to determine the relevance of corporate governance and IT governance to small businesses, and to define characteristics of IT governance in small businesses.

In the second part, a framework called ITGovSB will be developed and motivated. The framework will be based on the CobiT framework and the ISO/IEC 27002 information security controls.

Finally, the effectiveness of the framework will be evaluated by performing a case study at a small business.

1.6 Layout and conclusion

The treatise consists of eight chapters and one appendix. Figure 1.1 shows a graphic illustration of the layout of the chapters. The contents of the eight chapters will be summarised briefly.
Figure 1.1. Layout of chapters.
Chapter one provides background information and introduces the area that will be studied. The problem statement and the objectives that must be reached to solve the problem are presented, as well as the methodology that will be followed to achieve this.

In chapter two, small businesses will be discussed. The chapter will present background information on small businesses to reveal the factors that distinguish small businesses from larger organisations, such as forms of ownerships and management structures. The importance of small businesses to the economy as well as the problems they face will be discussed.

Chapter three addresses corporate governance. The benefits of corporate governance and the corporate governance guidelines in three different countries will be summarised. The objective of the chapter is to assess whether corporate governance applies to small businesses and can offer benefits to them.

Chapter four will cover IT governance. The reasons for implementing IT governance will be addressed, as well as three of the most widely used IT governance frameworks.

In chapter five, the relevance of IT governance in small businesses will be explored. After studying the differences between IT governance in small businesses and larger organisations, seven characteristics of IT governance in small businesses will be identified, motivated and presented.

The ITGovSB framework will be proposed in chapter six. The chapter will also evaluate the framework against the seven characteristics of IT governance that was presented in chapter five.

Chapter seven describes a case study. The purpose of the chapter is to examine the implementation of the framework at a small business and to determine the effectiveness thereof.
Chapter eight concludes the treatise by looking at the primary and secondary objectives and how they were achieved. A brief summary of each chapter will be provided, demonstrating how each chapter contributed towards achieving the objectives.
Chapter 2

Small Businesses

2.1 Introduction

2.2 What is a small business?

2.3 The importance of small businesses

2.4 Forms of ownership of small businesses

2.5 Management in small businesses

2.6 Problems facing small businesses

2.7 Conclusion
2.1 Introduction

What is a small business? At first, this might seem like a fairly straightforward question, but as one delves deeper into the topic, it becomes clear that the issue of what constitutes a small business may not be as simple as expected. This chapter will commence by attempting to answer this question and defining a small business in the context of this study.

Apart from defining a small business, the objective of this chapter is to provide some background information about small businesses to reveal the major factors that differentiate small businesses from larger organisations. Understanding the differences between small businesses and larger organisations is useful in gaining a better understanding of how small businesses fit into the subject area of corporate governance and, more specifically, IT governance.

Small businesses make a unique contribution to the economy of any country. In addition, there are many problems that they face. The importance of small businesses to the economy and the biggest problems faced by them will be addressed.

Small businesses can adopt many forms of ownerships, each with its own advantages and disadvantages. In this chapter, the various forms of ownerships and management structures will be discussed by looking at the characteristics of each and providing a brief comparison.

2.2 What is a small business?

This section will address the term “small business” by pointing out the difficulty of classifying businesses by size and by exploring how small businesses are classified in different countries and by various researchers. Finally, the different contexts that the term “small business” can be used in
will be addressed, and a small business will be defined for the purposes of this study.

Historically, all businesses were small and there was no need to classify businesses by size. This became necessary as economic activity flowed from owner-managed enterprises to managerial corporations (Fuller, 2003, p. 305). The issue of what constitutes a small or medium enterprise is a matter of concern in the SME literature (Abor & Adjasi, 2007, p. 112). The classification of firms by size varies among countries, researchers and other bodies. Some use the number of employees, some use capital asset, while others use turnover level. Some even define SMEs in terms of their legal status and method of production.

Not everyone agrees with the classification of businesses by size. Weston and Copeland (1998) hold the view that because enterprises may be conceived of in varying terms, the definitions of size of enterprises suffer from a lack of universal applicability. Storey (1985) tries to sum up the danger of using size to define the status of a firm by saying that in some sectors all firms may be regarded as small whilst in other sectors there are possibly no firms which are small. This issue is addressed in some of the definitions of a small business, as will be evident in the following sub-sections.

2.2.1 Classification in various countries

Different countries classify businesses by size differently. Most countries define small businesses in legislation for legal reasons and to assist in the issuing of loans and grants. The definition of a small business in South Africa, the United States and the United Kingdom will be addressed in this sub-section.

The South African National Small Business Act of 1996 (South Africa, 1996) defines a small business as “a separate and distinct business entity, including cooperative enterprises and non-governmental
<table>
<thead>
<tr>
<th>Sector or subsector in accordance with the Standard Industrial Classification</th>
<th>Size of class</th>
<th>Column 3: The total full-time equivalent of paid employees</th>
<th>Column 4: Total turnover (South Africa, 2003)</th>
<th>Column 5: Total gross asset value (fixed property excluded)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agriculture</td>
<td>Medium</td>
<td>100</td>
<td>R5m</td>
<td>R5m</td>
</tr>
<tr>
<td></td>
<td>Small</td>
<td>50</td>
<td>R3m</td>
<td>R3m</td>
</tr>
<tr>
<td></td>
<td>Very Small</td>
<td>10</td>
<td>R0.50m</td>
<td>R0.50m</td>
</tr>
<tr>
<td></td>
<td>Micro</td>
<td>5</td>
<td>R0.20m</td>
<td>R0.10m</td>
</tr>
<tr>
<td>Mining and Quarrying</td>
<td>Medium</td>
<td>200</td>
<td>R39m</td>
<td>R23m</td>
</tr>
<tr>
<td></td>
<td>Small</td>
<td>50</td>
<td>R10m</td>
<td>R6m</td>
</tr>
<tr>
<td></td>
<td>Very Small</td>
<td>20</td>
<td>R4m</td>
<td>R2m</td>
</tr>
<tr>
<td></td>
<td>Micro</td>
<td>5</td>
<td>R0.20m</td>
<td>R0.10m</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>Medium</td>
<td>200</td>
<td>R51m</td>
<td>R19m</td>
</tr>
<tr>
<td></td>
<td>Small</td>
<td>50</td>
<td>R13m</td>
<td>R5m</td>
</tr>
<tr>
<td></td>
<td>Very Small</td>
<td>20</td>
<td>R5m</td>
<td>R5m</td>
</tr>
<tr>
<td></td>
<td>Micro</td>
<td>5</td>
<td>R0.20m</td>
<td>R0.10m</td>
</tr>
<tr>
<td>Electricity, Gas and Water</td>
<td>Medium</td>
<td>200</td>
<td>R51m</td>
<td>R19m</td>
</tr>
<tr>
<td></td>
<td>Small</td>
<td>50</td>
<td>R13m</td>
<td>R5m</td>
</tr>
<tr>
<td></td>
<td>Very Small</td>
<td>20</td>
<td>R5.10m</td>
<td>R1.90m</td>
</tr>
<tr>
<td></td>
<td>Micro</td>
<td>5</td>
<td>R0.20m</td>
<td>R0.10m</td>
</tr>
<tr>
<td>Construction</td>
<td>Medium</td>
<td>200</td>
<td>R26m</td>
<td>R5m</td>
</tr>
<tr>
<td></td>
<td>Small</td>
<td>50</td>
<td>R6m</td>
<td>R1m</td>
</tr>
<tr>
<td></td>
<td>Very Small</td>
<td>20</td>
<td>R3m</td>
<td>R0.90m</td>
</tr>
<tr>
<td></td>
<td>Micro</td>
<td>5</td>
<td>R0.20m</td>
<td>R0.10m</td>
</tr>
<tr>
<td>Retail and Motor Trade and Repair Services</td>
<td>Medium</td>
<td>200</td>
<td>R39m</td>
<td>R6m</td>
</tr>
<tr>
<td></td>
<td>Small</td>
<td>50</td>
<td>R19m</td>
<td>R6m</td>
</tr>
<tr>
<td></td>
<td>Very Small</td>
<td>20</td>
<td>R4m</td>
<td>R0.60m</td>
</tr>
<tr>
<td></td>
<td>Micro</td>
<td>5</td>
<td>R0.20m</td>
<td>R0.10m</td>
</tr>
<tr>
<td>Wholesale Trade, Commercial Agents and Allied Services</td>
<td>Medium</td>
<td>200</td>
<td>R64m</td>
<td>R10m</td>
</tr>
<tr>
<td></td>
<td>Small</td>
<td>50</td>
<td>R32m</td>
<td>R5m</td>
</tr>
<tr>
<td></td>
<td>Very Small</td>
<td>20</td>
<td>R6m</td>
<td>R0.60m</td>
</tr>
<tr>
<td></td>
<td>Micro</td>
<td>5</td>
<td>R0.20m</td>
<td>R0.10m</td>
</tr>
<tr>
<td>Catering, Accommodation and other Trade</td>
<td>Medium</td>
<td>200</td>
<td>R13m</td>
<td>R3m</td>
</tr>
<tr>
<td></td>
<td>Small</td>
<td>50</td>
<td>R6m</td>
<td>R1m</td>
</tr>
<tr>
<td></td>
<td>Very Small</td>
<td>20</td>
<td>R5.10m</td>
<td>R1.90m</td>
</tr>
<tr>
<td></td>
<td>Micro</td>
<td>5</td>
<td>R0.20m</td>
<td>R0.10m</td>
</tr>
<tr>
<td>Transport, Storage and Communications</td>
<td>Medium</td>
<td>200</td>
<td>R26m</td>
<td>R6m</td>
</tr>
<tr>
<td></td>
<td>Small</td>
<td>50</td>
<td>R13m</td>
<td>R3m</td>
</tr>
<tr>
<td></td>
<td>Very Small</td>
<td>20</td>
<td>R3m</td>
<td>R0.60m</td>
</tr>
<tr>
<td></td>
<td>Micro</td>
<td>5</td>
<td>R0.20m</td>
<td>R0.10m</td>
</tr>
<tr>
<td>Finance and Business Services</td>
<td>Medium</td>
<td>200</td>
<td>R26m</td>
<td>R5m</td>
</tr>
<tr>
<td></td>
<td>Small</td>
<td>50</td>
<td>R13m</td>
<td>R3m</td>
</tr>
<tr>
<td></td>
<td>Very Small</td>
<td>20</td>
<td>R3m</td>
<td>R0.60m</td>
</tr>
<tr>
<td></td>
<td>Micro</td>
<td>5</td>
<td>R0.20m</td>
<td>R0.10m</td>
</tr>
<tr>
<td>Community, Social and Personal Services</td>
<td>Medium</td>
<td>200</td>
<td>R13m</td>
<td>R6m</td>
</tr>
<tr>
<td></td>
<td>Small</td>
<td>50</td>
<td>R6m</td>
<td>R3m</td>
</tr>
<tr>
<td></td>
<td>Very Small</td>
<td>20</td>
<td>R1m</td>
<td>R0.60m</td>
</tr>
<tr>
<td></td>
<td>Micro</td>
<td>5</td>
<td>R0.20m</td>
<td>R0.10m</td>
</tr>
</tbody>
</table>

Figure 2.1. Schedule referred to in the National Small Business Amendment Bill of 2003 (South Africa, 2003).
organisations, managed by one owner or more which, including its branches or subsidiaries, if any, is predominantly carried on in any sector or subsector of the economy mentioned in column I of the Schedule and which can be classified as a micro-, a very small, a small or a medium enterprise by satisfying the criteria mentioned in columns 3, 4 and 5 of the Schedule opposite the smallest relevant size or class as mentioned in column 2 of the Schedule”. The schedule referred to in the definition has since been substituted by an updated schedule (Figure 2.1) in the National Small Business Amendment Bill of 2003 (South Africa, 2003).

Judging by the number of employees, a small enterprise, according to the schedule, is one with a maximum of 50 employees no matter in what industry the business operates. The turnover and asset value differ quite considerably by industry.

The definition used by the United States Congress in the US Small Business Act of 1953 (US Small Business Administration, 2008) states that “a small business is one that is independently owned and operated and is not dominant in its field of operation”. The US Small Business Administration (SBA) uses different size criteria by industry. In general, however, it uses the size classification shown in Figure 2.2.

<table>
<thead>
<tr>
<th></th>
<th>Under 20 employees</th>
<th>20–99</th>
<th>100–499</th>
<th>500 or more</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>Very small</td>
<td>Small</td>
<td>Medium</td>
<td>Large</td>
</tr>
</tbody>
</table>

Source: Small Business Administration.

Figure 2.2. Classification of business by size according to the SBA (Megginson, Byrd & Megginson, 2006).

In the United Kingdom, the term “small business” originated in 1969 with the establishment of the Bolton Committee. They defined small businesses based on their inherent characteristics, i.e. the business is
independently owned and managed by its owners or part owners and that it has a small market share (Fuller, 2003, p. 306).

In 1996, the European Community defined a small enterprise for statistical purposes as one that is independently owned and has fewer than 50 employees, with maximum sales of €7 million or capitalisation of €5 million (Fuller, 2003, p. 306).

These classifications vary considerably by country. To get an even better appreciation of the diversity of the definitions of small businesses, it is necessary to look at the classification of business sizes by various researchers as well.

2.2.2 Classification by various researchers

The classification of businesses by size varies noticeably among researchers. It also depends on the type of study undertaken. Most researchers, however, use the number of employees to define businesses by size.

Brouthers, Andriessen and Nicolaes (1998, p. 130) define a small firm as one with fewer than 100 employees. Van der Wijst (1989) considers small and medium-sized businesses as privately held firms with one to nine and ten to 99 people employed, respectively. Jordan, Lowe and Taylor (1998) define SMEs as firms with fewer than 100 employees and a turnover below €15 million. Michaelas, Chittenden and Poutziouris (1999) consider small, independent, private limited companies with fewer than 200 employees and López and Aybar (2000) analyse companies with sales below €15 million.

Although it is the most frequently used method, not all researchers classify small businesses according to the number of employees or the turnover. Fuller (2003, p. 307) uses the definition of the Bolton...
Committee as a guide by defining a small business as “one that is owned by the people running it and which is relatively powerless with respect to a national or global market.” Verhees and Meulenberg (2004, p. 135) define a small firm as one that is run and is controlled under the direct supervision of the owner.

2.2.3 The term “small business” in different contexts

As can be seen from the definitions in the previous sub-sections, the terms “small business”, “small enterprise” and “small and medium-sized enterprise” can create some confusion. This is because the term “small business” is being used in two different contexts. The first context (Context 1) is similar to the one used in the South African National Small Business Act of 1996 (South Africa, 1996), where the terms “micro-, very small, small and medium enterprises” all fall under the heading of “small business”. In this context, the term SME would, therefore, fall under “small business”, which does create confusion. In the second context (Context 2), the term “small business” means a small enterprise. Figure 2.3 attempts to provide clarity on the issue by showing the relationship between the various contexts in a hierarchy.

![Figure 2.3. The term “small business” in different contexts.](image-url)
This section reviewed a number of the many available definitions of small businesses. After considering definitions from various countries and researchers, it is clear that the classification of businesses by size and the size of small businesses in different definitions vary quite dramatically. For the purposes of this study, which uses the South African National Small Business Act of 1996 (South Africa, 1996) as a guide, a small business (or small enterprise) means one with 50 employees or less.

The lack of universal definitions for small businesses can partly be contributed to the great number of small businesses that form part of the economy. In the next section, the contribution that the many small businesses make to the world economy will be addressed.

2.3 The importance of small businesses

The value of goods and services that the small business sector produces and the new jobs it creates make it one of the greatest economic powers in the world. In this section, the importance of small businesses and the unique contribution that they make to the economy will be addressed.

According to the SBA (Megginson et al., 2006, p. 5), there are about 23 million small businesses in the United States. They create 75 percent of new jobs and employ 50 percent of the country’s private work force. They also represent more than 99 percent of all employers and 97 percent of exporters. In the European Union, SMEs provide employment relating to two thirds of all jobs. In Japan, 78 percent of jobs are provided by such firms (Bernroider, 2002, p. 563).

Megginson et al. (2006, p. 9) sum up some of the unique contributions of small businesses. They:

- encourage innovation and flexibility,
- maintain close relationships with customers and the community,
• keep larger firms competitive,
• provide employees with comprehensive learning experiences,
• develop risk takers,
• generate new employment, and
• provide greater job satisfaction.

Small businesses play a vital role in the economy of any country. Not only do they provide employment to the bulk of the workforce in most countries, but they make a unique contribution that is hard to imitate by larger organisations.

The number of small businesses and their variation in business size and ownership make it impossible for all small businesses to have the same structure. In the next section, the various forms of ownership that small businesses can adopt will be explored.

2.4 Forms of ownership of small businesses

This section will address the types of business that are most common for small businesses to take on by summarising what each type of business entails, as well as its main advantages and disadvantages.

2.4.1 Sole proprietors

This sub-section will address sole proprietors. A sole proprietor is a business owned by one person. In the United States it is often called a proprietorship and in the United Kingdom it is referred to as a sole trader.

Sole proprietors own all assets of the business and the profits generated by it. They also assume complete responsibility for any of its liabilities or debts. In the eyes of the law and the public, the sole proprietor is one and the same with the business. It is the oldest and
most prevalent form of ownership, as well as the least expensive to start. Most small business owners prefer the proprietorship because it is simple to enter, operate and terminate and provides for relative freedom of action and control. In addition, the sole proprietor has a favourable tax status. It is taxed at the owner’s personal income tax rate (Megginson et al., 2006, p. 57).

Sole proprietors also have some negative factors. From a legal point of view, the business and its owner are one and the same and cannot be separated. Consequently, the business legally ends with the proprietor’s death, and some legal action must be taken to restart it. Also, if the business does not have enough funds to pay its obligations, the owner must use personal assets to pay them (Megginson et al., 2006, p. 57).

2.4.2 Partnerships

Whereas a sole proprietor is a business owned by one person, a partnership is a voluntary association of two or more persons to carry on as co-owners of a business for profit. In a partnership, two or more people share ownership of a single business.

Like sole proprietors, the law does not distinguish between the business and its owners. The partners should have a legal agreement that sets out how decisions will be made, how profits will be shared, how disputes will be resolved, how future partners will be admitted to the partnership, how partners can be bought out, and what steps will be taken to dissolve the partnership when needed. They must also decide up front how much time and capital each will contribute. The partnership is similar to the sole proprietor but is more difficult to form, operate and terminate. As with the sole proprietor, profits are taxed only once – on each partner’s share of the income (Megginson et al., 2006, p. 58).
Unlike a sole proprietor or partnership, independent legal entities are businesses that are separate from its members. This type of business will be addressed in the next sub-section.

2.4.3 Independent legal entities

Independent legal entities are businesses that are separate from the members or shareholders who own it. The continued legal existence of the entity is, therefore, not influenced by any change in membership. Because the law sees such a business as separate from its members, the assets and debts of the business, unlike a sole proprietor or partnership, belong to the business and have nothing to do with the assets and debts of the members or shareholders.

Many of the definitions of small businesses in section 2.2 refer to businesses that are independently owned. Just as the definition of small businesses varies, the types and names of independently owned businesses vary by country. It will, therefore, be useful to look at the different forms of ownership of these businesses in South Africa, the United States and the United Kingdom.

Independent legal entities in South Africa

In South Africa, an independent legal entity can be a close corporation (CC), a private company or a public company.

A close corporation is like a company, only less expensive and less complicated to run. The people who own and manage the close corporation are called members. There are no directors or shareholders or a chairperson of the board, like a company has. A close corporation cannot have more than ten members (Paralegal, 2008, p. 489).
A close corporation is more expensive to run than a partnership or sole proprietorship because an accounting officer needs to do the books of the business. The members also have to keep records of the close corporation and each member has to keep records for tax purposes. Therefore, it is only recommended to register a close corporation if it is very important to have limited liability, remembering that banks and suppliers could still ask the members to sign surety (Paralegal, 2008, p. 489).

If more than ten people want to start a business together with limited liability, they will have to form a company. A company has shareholders and directors (Paralegal, 2008, p. 490). The shareholders own the company and appoint the directors to run it on their behalf (Swiftreg, 2008). Companies have to adhere to all the rules of the Company Act of 1973, which is a lengthy and complex law.

A private company cannot have more than 50 shareholders and its shares may not be offered to the general public. If a shareholder wants to sell any shares, he has to offer it to another shareholder in the same company. A private company does not have to lodge interim reports and its annual reports are not available to the public (Swiftreg, 2008).

A public company can have any number of shareholders and the shares can be freely traded. For this reason, quarterly reports and annual financial statements have to be lodged with the Companies and Intellectual Property Registration Office (CIPRO), where they become available for public inspection. Public companies are usually listed on the Johannesburg Securities Exchange (JSE) (Swiftreg, 2008).

**Independent legal entities in the United States**

In the United States, the most common forms of ownership for businesses that are independently owned are the corporation, S
corporation and limited-liability company.

The traditional form of the corporation is called a C corporation. A corporation is considered by law to be a unique entity, separate and apart from those who own it. A corporation can be taxed, sued and it can enter into contractual agreements. The owners of a corporation are its shareholders. The shareholders elect a board of directors to oversee the major policies and decisions. The corporation has a life of its own and does not dissolve when ownership changes.

The corporation offers several advantages. Because it is separate and distinct from the owners as individuals, the death of one shareholder does not affect the “life” of the corporation. Also, each owner’s liability for the firm’s debt is limited to the amount invested, so personal property cannot be taken to pay the debts of the business (with certain limited restrictions, such as loan guarantees and non-payment of taxes).

The main disadvantage of a corporation is double taxation, as the corporation pays taxes on its profit, and then individual owners pay taxes on their dividends.

The S corporation is a special type of corporation that is exempt from multiple taxation and excessive paperwork. Any business with fewer than 75 shareholders, none of whom are corporate shareholders, can apply to form such a corporation.

The limited-liability company combines the advantages of a corporation, such as liability protection, with the benefits of a partnership, such as tax advantages. Limited-liability companies provide benefits similar to the S corporation, without the special eligibility requirements.
Independent legal entities in the United Kingdom

In the United Kingdom, a private limited company and public limited company can be compared to a private company and public company in South Africa.

The limited liability, potential tax advantages, and simplicity of running a private limited company make this the most common form of registered business in the United Kingdom. In addition to limited liability, this form of company is also considered to be more prestigious by other companies and the general public due to its legitimate nature and the way important information is recorded at Companies House. Anyone wishing to conduct business with a limited company can verify who is connected to the company and also the financial position of the company by paying Companies House a small fee (Simple Formations, 2008).

A public limited company differs from a private limited company in that it is able to sell its shares to the public, and may be quoted on a stock exchange or alternative investment market. A public company must satisfy Companies House that at least £50,000 worth of shares have been issued before it is entitled to begin business or borrow money, and two directors must be appointed. The cost of running a public limited company is considerably higher, and so this form of business is better suited to large organisations (Simple Formations, 2008).

Having reviewed the different types of ownership that small businesses can take on, it will be useful to compare them against one another. Megginson et al. (2006, p. 55) provide a comparison of the popularity, revenue and profit between proprietorships, partnerships and corporations in the United States.

The proprietorship is by far the most popular form of business, as can be seen
in Figure 2.4. Around 72 percent of all businesses are proprietorships, while only 20 percent are corporations and eight percent partnerships. Notice in Figure 2.5 that the proprietorship is most popular in all industries. Finance, insurance and real estate use partnership more frequently than do the other industries.

<table>
<thead>
<tr>
<th>A. Proprietorships are the most numerous.</th>
<th>B. Corporations produce the most revenue.</th>
<th>C. Proprietorships appear more profitable.</th>
</tr>
</thead>
<tbody>
<tr>
<td>8%</td>
<td>4.5%</td>
<td>15%</td>
</tr>
<tr>
<td>20%</td>
<td>10%</td>
<td>19%</td>
</tr>
<tr>
<td>72%</td>
<td>85.5%</td>
<td>66%</td>
</tr>
</tbody>
</table>

Distribution by total number

Distribution by revenues

Distribution by profits

Figure 2.4. Relative position of United States proprietorships, partnerships and corporations (Megginson et al., 2006).

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage of Firms in the Industry</th>
<th>Percentage of Industry's Business in Receipts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Proprietorships</td>
<td>Partnerships</td>
</tr>
<tr>
<td>Services</td>
<td>76</td>
<td>4</td>
</tr>
<tr>
<td>Trade</td>
<td>70</td>
<td>4</td>
</tr>
<tr>
<td>Construction</td>
<td>78</td>
<td>3</td>
</tr>
<tr>
<td>Finance, insurance, real estate</td>
<td>44</td>
<td>34</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>52</td>
<td>6</td>
</tr>
</tbody>
</table>

*Less than 1 percent.


Figure 2.5. Comparison of proprietorships, partnerships and corporations in selected industries (Megginson et al., 2006).

While the proprietorship is the most popular form of business, it accounts for
only a small share of total revenues. As Figure 2.4 shows, proprietorships generate only around five percent of all revenues, while corporations account for about 85 percent and partnerships provide around ten percent.

Figure 2.4 shows that proprietorships appear to be the most profitable form. They received 15 percent of profits on only about five percent of revenues. Partnerships accounted for eight percent of revenues and 19 percent of profits. Corporations received only 66 percent of profits on about 86 percent of the sales. These numbers should be interpreted with caution, however, because proprietorship “profits” include net financial return to owners. In a corporation, much of that return would be included in wage and salary expense and deducted from profit.

This section addressed the various forms of ownership available to small businesses and provided a comparison between proprietorships, partnerships and corporations. While a proprietorship is the most popular form and appear the most profitable, corporations generate by far the most revenue. Business ownership plays a role in the structure and management model that a business will adopt. In the next section, management models in the context of small businesses will be discussed.

2.5 Management in small businesses

Management theories that have been developed for and applied to larger organisations are difficult to replicate in small businesses. New models are necessary for the distinctive conditions facing small firms (Beaver & Prince, 2004, p. 35).

Apart from size, business ownership is the key feature that differentiates the management of small businesses from that of large organisations. Ownership of large organisations is normally distanced from management, which is not the case in the majority of small businesses (Beaver & Prince, 2004, p. 35).
In an international survey by Groupe ESC Rennes (Hankinson, Bartlett & Ducheneaut, 1997, p. 170), owner-managers of small SMEs were offered two management models for consideration (Figure 2.6). Almost 90 percent of the respondents opted for model two, which has one hierarchical level in the management structure. The remaining ten percent that consisted of two or three levels tended to be larger companies.

![Figure 2.6. Management models (Hankinson et al., 1997).](image)

Just as small businesses are unique in terms of business ownership and management, they face a distinct set of problems. In the next section the most common problems that face small businesses will be addressed.

### 2.6 Problems facing small businesses

In this section, the business-related problems facing small businesses will be discussed. Small businesses also face many IT-related issues, which will be discussed in chapter five.

Megginson et al. (2006, p. 12) identified areas that create problems for small businesses. These areas include:

- Inadequate financing. Inadequate financing is the primary cause of new business failure. A shortage of capital is the greatest problem facing small business owners.
• Inadequate management. Inadequate management, in the form of limited business knowledge, poor management, inadequate planning and inexperience, is the second problem facing small businesses. Many owners tend to rely on one-person management and seem reluctant to vary from this managerial pattern.

• Burdensome government regulations and paperwork. In the past, small businesses were exempt from many government regulations. Now, they are subject to many of the same regulations as their larger competitors. These regulations are often complex and contradictory, which explains why small business managers find it so difficult to comply with government requirements.

In a 2004 survey by the NFIB Research Foundation (Phillips, 2004, p. 5), the most severe problems for small-business owners in the United States were noted. The problems included cash flow, unreasonable government regulations, energy and electricity costs, property taxes and taxes on business income.

It is evident that of all the problems facing small businesses, a lack of funding is the biggest cause of distress for small business owners. Government regulations are also a concern, as many of the regulations that are intended for larger organisations affect small businesses inherently.

2.7 Conclusion

Different countries and researchers use various ways of classifying businesses by size and defining a small business. Because not all definitions use the same criteria, it is not possible to identify one such definition as the best. At best, the meaning of a small business in the context of this study can be defined. For this purpose, a small business will mean any business with 50 employees or less.
Small businesses play an important part in the economy. In many countries, most of the workforce is employed by small businesses. Apart from keeping larger organisations competitive, they provide contributions that are difficult to match by larger organisations, such as encouraging innovation and flexibility and providing better job satisfaction.

Just as small businesses offer unique contributions, they also face problems that are more applicable to such businesses. Financial problems and government regulations tend to be high on the list from a business perspective.

Although the forms of ownership of small business vary by country, most small businesses can be categorised as either a sole proprietor, partnership, or an independent legal entity. The type of business is determined mostly by the size of the business, the number of owners or shareholders, and other requirements such as limited liability.

This chapter provided a brief background of small businesses and in the process identified certain factors that distinguish small businesses from larger organisations. These differences make it easier to understand why certain concepts, as in the case of this study, IT governance, cannot be applied to small businesses in exactly the same way as they are applied to larger organisations.

IT governance is a component of corporate governance. Before addressing IT governance in small businesses, it is, therefore, imperative to obtain a good understanding of corporate governance and how it relates to small businesses. In the next chapter, corporate governance as a whole, as well as in the context of small businesses, will be analysed. Many of the problems facing small businesses can also be mitigated by applying good governance techniques.
Chapter 3

Corporate Governance

3.1 Introduction
3.2 What is corporate governance?
3.3 Why corporate governance?
3.4 Who is responsible for corporate governance?
3.5 Corporate governance standards
3.6 Corporate governance in small businesses
3.7 Conclusion
3.1 Introduction

Chapter two presented background information about small businesses and identified factors that distinguish small businesses from larger organisations. Corporate governance is a subject that is normally only associated with large organisations. The purpose of this chapter is to assess whether corporate governance applies, and can offer benefits, to small businesses as well. In order to achieve this, it is important to have a good understanding of corporate governance.

Corporate governance can be thought of as the system that is used to control organisations and it addresses the roles and interests of all stakeholders, including directors, shareholders, management and the community. This chapter will commence by considering a number of definitions and other characteristics in order to gain a clear understanding of what corporate governance is.

Corporate governance has been a topic of much discussion in recent years. In this chapter, the reasons for this will be discussed, as well as the reasons why an organisation would benefit from implementing good corporate governance.

There are a number of standards or best practices for implementing corporate governance. These standards vary by country or region. The corporate governance standards applicable to South Africa, the United States and the United Kingdom will be examined.

Although corporate governance has traditionally been associated with larger companies, it can be argued that such guidelines can be of great value for small businesses as well. This chapter concludes by considering this argument and addresses various ways for small businesses to benefit from the guidelines provided by corporate governance.
3.2 What is corporate governance?

This section will focus on what corporate governance is, and the systems and processes it is comprised of. Finally, the characteristics of good corporate governance will be addressed.

Corporate governance is the system by which companies are directed and controlled (Cadbury Committee, 1992, p. 15) and is concerned with holding the balance between economic and social goals and between individual and communal goals (King Committee, 2002, p. 6). While management can be seen as running an organisation, governance is about making sure that the organisation is run properly (Naidoo, 2002, p. 1).

Corporate governance consists of a number of systems, processes and practices to ensure that organisations are controlled effectively. They include a system of checks and balances to ensure a balanced exercise of power, a system to ensure compliance with legal and regulatory obligations, systems and processes to identify and manage risk to the company, and practices which make and keep the company accountable to the broader society in which it operates (Naidoo, 2002, p. 1). Organisations that are controlled effectively and apply good corporate governance share certain characteristics:

1. Discipline. Corporate discipline is described as a commitment by a company’s senior management to adhere to behaviour that is universally recognised and accepted to be correct and proper.

2. Transparency. Transparency is the ease with which an outsider is able to make meaningful analysis of a company’s actions, its economic fundamentals and the non-financial aspects pertinent to that business. It reflects whether or not investors obtain a true picture of what is happening inside the company.
3. Independence. This is the extent to which mechanisms have been put in place to minimise or avoid potential conflicts of interest that may exist, such as dominance by a strong chief executive or large shareowner. These mechanisms range from the composition of the board, to appointments to committees of the board, and external parties such as the auditors.

4. Accountability. Individuals or groups in a company, who make decisions and take actions on specific issues, need to be accountable for their decisions and actions. Mechanisms must exist and be effective to allow for accountability. These mechanisms provide investors with the means to query and assess the actions of the board and its committees.

5. Responsibility. With regard to management, responsibility pertains to behaviour that allows for corrective action and for penalising mismanagement. While the board is accountable to the company, it must act responsively to and with responsibility towards all stakeholders of the company.

6. Fairness. The systems that exist within the company must be balanced in taking into account all the stakeholders and its future. The rights of these stakeholders have to be acknowledged and respected.

7. Social responsibility. A well-managed company will be aware of, and respond to, social issues, placing a high priority on ethical standards. A good corporate citizen is increasingly seen as one that is non-discriminatory, non-exploitative, and responsible with regard to environmental and human rights issues.

This section addressed corporate governance and the characteristics of good corporate governance. The next section will emphasise why it is necessary for organisations to apply corporate governance and to ensure that they incorporate these characteristics.
3.3 Why corporate governance?

Until recently, not all organisations were aware of the risks of not applying good governance techniques. However, because of corporate governance malpractices such as the scandals of Enron and WorldCom, and the dramatic decline of stock markets at the beginning of the new century, the subject of corporate governance has received much attention recently (Letza et al., 2008, p. 17).

The primary reason corporate governance principles were developed was because investors were worried about the excessive concentration of power in the hands of management. Markets exist by the grace of investors, and if the investors are not confident with the level of disclosure, capital will flow elsewhere (King Committee, 2002, p. 9).

The implications for organisations are profound. Simply by developing good governance practices, they can potentially add significant shareholder value. Several studies have indicated that institutional investors are willing to pay a premium of up to 27% for the shares of a well-governed organisation over one that is poorly governed, even if they have comparable financial records (Naidoo, 2002, p. 4).

One of the reasons that discourage organisations to consider corporate governance is the fact that it is not always easy to measure the effectiveness of corporate governance. One of the difficulties has been to provide satisfactory empirical evidence that good corporate governance pays. However, in its Investor Opinion Survey published in June 2000, McKinsey & Co. found that good governance could be quantified and was significant. Other similar surveys support the contentions put forward by McKinsey (King Committee, 2002, p. 12).

The proper governance of companies is crucial. If there is a lack of good corporate governance in a market, capital will leave that market very quickly.
The next section will continue by looking at the parties responsible for corporate governance in an organisation.

3.4 Who is responsible for corporate governance?

In this section the responsibilities of the board of directors, the management and the shareholders pertaining to corporate governance will be discussed.

According to the Cadbury Committee (1992, p. 14), boards of directors are responsible for the governance of their companies. The responsibilities of the board include setting the company’s strategic aims, providing the leadership to put them into effect, supervising the management of the business and reporting to shareholders on their stewardship.

Other parties in corporate governance include the shareholders and the management of the organisation. The shareholders’ role in governance is to appoint the directors and the auditors and to satisfy themselves that an appropriate governance structure is in place (Cadbury Committee, 1992, p. 14). Management’s role is to manage the organisation and to implement the strategy developed by the board.

Ultimately, the board of directors is responsible for implementing corporate governance. Many best practices are available to assist them with this responsibility. A number of these best practices will be presented in the next section.

3.5 Corporate governance standards

Companies are governed within the framework of the laws and regulations of the country in which they operate. Communities and countries differ in their culture, regulation, law and generally the way business is done (King Committee, 2002, p. 14). This section attempts to summarise the corporate
governance standards and best practices of South Africa, the United States and the United Kingdom.

3.5.1 The King Report on Corporate Governance

The King Committee was formed in 1992 to consider corporate governance in the context of South Africa. Corporate governance in South Africa was institutionalised by the publication of the King Report on Corporate Governance (King Report) in November 1994.

The purpose of the King Report was, and remains, to promote the highest standards of corporate governance in South Africa. Unlike its counterparts in other countries at the time, the King Report went beyond the financial and regulatory aspects of corporate governance in advocating an integrated approach to good governance in the interests of a wide range of stakeholders, having regard to the fundamental principles of good financial, social, ethical and environmental practice (King Committee, 2002, p. 6).

The King Report on Corporate Governance 2002 (King II Report) is the second report of the King Committee. While the committee remains firmly committed to the governance concepts of the King Report, a number of developments have taken place since its advent in November 1994. Consequently, the committee considered it appropriate to review corporate governance standards and practices for South Africa.

These developments since 1994 are outlined below:

- Some of recommendations contained in the King Report have been superseded by legislation in the social and political transformation that coincided with its release. Some of the more significant have been the Labour Relations Act (No. 66 of 1995),

- Other legislative developments since the publication of the King Report include the introduction of the Insider Trading Act (No. 135 of 1998) providing for more rigorous supervision and monitoring of insider trading, the Public Finance Management Act (No. 1 of 1999) bringing into force more stringent provisions for reporting and accountability, and a comprehensive update of the provisions and regulations governing the Banks Act (No. 94 of 1990) (King Committee, 2002, p. 8).

- The intervening period has also seen the listings requirements of the JSE Securities Exchange South Africa (JSE) comprehensively revised in 1995 and again in 2000 to ensure that they remain current with international best practice (King Committee, 2002, p. 8).

- A dominant feature of business since 1994 has been the emergence of information technology, in all its facets, as a key driver of business strategy and decisions (King Committee, 2002, p. 8).

The King II Report presents a code of corporate practices and conduct. The code applies to:

- All companies with securities listed on the JSE Securities Exchange.
• Banks, financial and insurance entities as defined in the various legislation regulating the South African financial services sector.

• Public sector enterprises and agencies that fall under the Public Finance Management Act and the Local Government: Municipal Finance Management Bill (still to be promulgated).

The code consists of seven sections that describe different areas of corporate governance:

1. Boards and Directors,
2. Risk Management,
3. Internal Audit,
4. Integrated Sustainability Reporting,
5. Accounting and Auditing,
6. Relations with Shareowners, and
7. Communication.

This sub-section summarised the South African approach to corporate governance. The two King reports focus not only on the financial and regulatory aspects of corporate governance, but take into account a wider range of stakeholders by focusing on the financial, social, ethical and environmental aspects.

3.5.2 The Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act of 2002 is the single most significant piece of legislation embracing corporate governance since the US securities laws of the 1930s (Riotto, 2007, p. 9). At the forefront of this legislation was the intention to restore public confidence and interest at a time when there were a number of corporate scandals. A brief overview of the act will be given in this sub-section.
The act was passed on 30 July 2002. It was sponsored by US senator Paul Sarbanes and US representative Michael Oxley, and signed into law by President George Bush. The act established new substantive and procedural requirements for public companies, their officers and directors with the intent to improve financial reporting, disclosure and restore public trust. The act’s objectives were to re-establish corporate governance. The majority of the act’s sections were targeted at solving certain shortcomings in auditing, corporate governance, and capital markets (Riotto, 2007, p. 2).

Although there are a number of controversial sections in the act that have created debate, comments and objections, sections 302 and 404 create the most radical, ongoing and potentially burdensome compliance obligations (Leech, 2003, p. 1). Simply put, these sections require that the CEO and CFO of an organisation certify and assert to stakeholders that SEC disclosures, including the financial statements of the company and all supplemental disclosures, are truthful and reliable, and that management has taken appropriate steps to satisfy themselves that the disclosure processes and controls in the company they oversee are capable of consistently producing financial information stakeholders can rely on (Section 302). The company’s external auditor must report on the reliability of management’s assessment of internal control (Section 404) (Leech, 2003, p. 5).

The act consists of 11 titles:

1. Title I - Public company accounting oversight board
2. Title II - Auditor independence
3. Title III - Corporate responsibility
4. Title IV - Enhanced financial disclosures
5. Title V - Analyst conflicts of interest
6. Title VI - Commission resources and authority
7. Title VII - Studies and reports
8. Title VIII - Corporate and criminal fraud accountability
9. Title IX - White collar crime penalty enhancements
10. Title X - Corporate tax returns
11. Title XI - Corporate fraud accountability

This sub-section summarised the Sarbanes-Oxley Act of 2002. The act was passed to re-establish confidence in corporate governance in the United States following a number of corporate scandals. Corporate governance in the United Kingdom was also re-addressed following similar scandals.

3.5.3 The Combined Code

Following a series of corporate collapses and scandals in the late 1980s and early 1990s, the development of corporate governance in the United Kingdom commenced with the setting up of the Committee on the Financial Aspects of Corporate Governance in 1991 (Financial Reporting Council, 2006, p. 3). Chaired by Sir Adrian Cadbury, the committee issued a series of recommendations, known as the Cadbury Report, in 1992. The Cadbury Report addressed issues such as the relationship between the chairman and chief executive, the role of non-executive directors and reporting on internal control and on the company's position. A requirement was added to the listing rules of the London Stock Exchange that companies should report whether they had followed the recommendations or, if not, explain why they had not done so (this is known as “comply or explain”) (Financial Reporting Council, 2006, p. 4).

The recommendations in the Cadbury Report have been added to at regular intervals since 1992. In 1995, the Greenbury Report set out recommendations on the remuneration of directors. In 1998, the Cadbury and Greenbury reports were brought together and updated in the Combined Code, and in 1999, the Turnbull guidance was issued to
provide directors with guidance on how to develop a sound system of internal control (Financial Reporting Council, 2006, p. 4).

Following the corporate scandals in the United States, the Combined Code was updated in 2003 to incorporate recommendations from reports on the role of non-executive directors (the Higgs Report) and the role of the audit committee (the Smith Report). At this time, the United Kingdom government confirmed that the Financial Reporting Council (FRC) was to have the responsibility for publishing and maintaining the Code. The FRC made further, limited, changes to the Code in 2006. Throughout all of these changes, the “comply or explain” approach, first set out in the Cadbury Report, has been retained (Financial Reporting Council, 2006, p. 4).

The Combined Code identifies good governance practices relating to, for example, the role and composition of the board and its committees and the development of a sound system of internal control, but companies can choose to adopt a different approach if that is more appropriate to their circumstances. Where they do so, however, they are required to explain the reason to their shareholders, who must decide whether they are satisfied with the approach that has been taken (Financial Reporting Council, 2006, p. 6).

This framework is reinforced by the Listing Rules that must be followed by companies listed on the Main Market of the London Stock Exchange (Financial Reporting Council, 2006, p. 7). The Listing Rules provide further rights to shareholders and require certain information to be disclosed to the market.

The essential features of corporate governance in the United Kingdom are (Financial Reporting Council, 2006, p. 9):

- The role and composition of the board,
• Remuneration,
• Accountability and audit, and
• Relations with shareholders.

This sub-section examined corporate governance in the United Kingdom. Since initiating the development of corporate governance in the United Kingdom in 1992, the Cadbury Report has been updated and combined with various other reports to form the Combined Code.

In this section, corporate governance approaches in South Africa, the United States and the United Kingdom were summarised by reviewing the King Report on Corporate Governance, the Sarbanes-Oxley Act of 2002, and the Combined Code. Having looked at the different approaches, and given differences in culture, laws and regulations in different countries and communities, it is clear that there can be no single, generally applicable corporate governance standard. Yet, there are international standards that no country can ignore in the era of the global investor. Thus, international guidelines have been developed by the Organisation for Economic Co-operation and Development (OECD), the International Corporate Governance Network, and the Commonwealth Association for Corporate Governance. The four primary pillars of fairness, accountability, responsibility and transparency are fundamental to all these international guidelines of corporate governance (King Committee, 2002, p. 14).

One can be forgiven for assuming that corporate governance only applies to large organisations and not to small businesses with fewer employees and simpler management structures. In the next section the relevance of corporate governance in small businesses will be addressed.

3.6 Corporate governance in small businesses

Corporate governance has traditionally been associated with larger organisations. This is mainly due to the separation between ownership and
control of the firm. In this section, corporate governance as pertaining to small businesses will be discussed.

It is tempting to believe that corporate governance would not apply to small businesses since agency problems are less likely to exist. Basically, small businesses tend to have a less distinct separation of ownership and management than larger organisations. Also, the question of accountability by small businesses to the public is non-existent since they do not depend on public funds (Abor & Biekpe, 2007, p. 290).

In spite of these arguments, there is a global concern for the application of corporate governance to small and medium-sized enterprises. It is often argued that similar guidelines that apply to listed companies should also be applicable to such enterprises. In the next sub-section the reasons for this argument will be addressed.

3.6.1 Benefits of corporate governance in small businesses

In this sub-section, the benefits that corporate governance can offer small businesses will be explored.

Corporate governance can greatly assist the small business sector by infusing better management practices, stronger internal auditing, greater opportunities for growth and new strategic outlooks through non-executive directors. Good governance mechanisms among small businesses are likely to result in boards exerting much-needed pressure for improved performance by ensuring that the interests of the business are served (Abor & Biekpe, 2007, p. 296).

One major implication of a well-functioning corporate governance system is easier access to funding from investors and financial institutions. Small businesses, generally, encounter greater difficulty in gaining access to financing due to problems of information
asymmetry and moral hazards. Ensuring proper accounting practices, internal control systems and adequate information disclosure is likely to increase the confidence of investors in the business, reduce the problems associated with information asymmetry and make the business less risky to invest in. The presence of external supervisory parties and monitoring systems could also limit the problem of moral hazard by discouraging entrepreneurs from redirecting borrowed funds to invest in unapproved projects (Abor & Biekpe, 2007, p. 296).

The existence of non-executive directors could lead to better management decisions and help small businesses to attract better resources. Also, non-executive directors may have good knowledge or useful information on financing facilities. Small businesses are particularly weak and often ignorant of sources of finance open to their firms. Most of the time, they do not know how to position themselves correctly to be viewed favourably by these sources of finance providers. The infusion of external board membership in this case is crucial since there is a high incentive for the board members to introduce ways of attracting finance (Abor & Biekpe, 2007, p. 297).

Small businesses need access to resources for growth. They need inputs on business operations, good strategy and best practices in the industrial sector. These resources can be provided for through the presence of non-executive directors. Research on listed firms has shown that strategy influences corporate performance and external board members challenge strategies by management (Abor & Adjasi, 2007, p. 117). Thus, the existence of external board members could lead to better management decisions and help small businesses to attract better resources. Non-executive directors could also introduce creativity and innovation through opinions and suggestions during decision-making. In the Japan Small Enterprise Agency, small and medium-sized enterprises with very high growth rates use non-
executive directors more actively than larger organisations (Abor & Adjasi, 2007, p. 117).

Corporate governance also allows businesses to prepare for their pending initial public offering. Often businesses seeking new funds find that they have much work to do before confidently going to the market. A consistent track record of good governance will greatly assist when that point comes. The existence of a board will induce rapid growth strategies in the business for rapid profits. This will, at a point, require the firm going public for more finances. Thus, the transition from a small to medium and, finally, large organisation could be smoothly aided by an effective corporate governance system (Abor & Biekpe, 2007, p. 290).

The existence of a board of directors plays a vital role in corporate governance. Many of the benefits that small businesses can achieve from corporate governance involve the board of directors. In the next sub-section, boards of directors and the role they play in small businesses will be addressed.

3.6.2 Boards of directors in small businesses

Because large public companies recognise the value to the corporation and because of the increased regulatory requirements placed on publicly traded companies, the use of boards of directors are strongly endorsed. For small businesses and privately held companies, however, a board of directors is not always viewed as a useful part of the corporate structure (Teksten, Moser & Elbert, 2005, p. 50). Reasons include fewer regulatory governance requirements or perhaps the closer relationship between managers and owners (Teksten et al., 2005, p. 52).
An alternative to diversifying the board of an organisation is to seek inputs from outside sources of expertise through advice and consultancy. This can be for filling once off gaps in specialist skills, continuing advisory relationships, or transferring expertise to the owners or managers through training and development (Bennett & Robson, 2004, p. 99).

Although small businesses often do not have boards of directors, there are, as was discussed in the previous sub-section, many advantages to having a board of directors. In small businesses, the role of directors is different from and more direct than in large organisations. Bennett and Robson (2004, p. 96) discuss three main theories that link board roles and business performance:

1. Resource dependence,
2. Counselling, and
3. Control.

Each of these theories reinforces the fact that the role of boards of directors differs between small businesses and larger organisations.

The resource dependence approach emphasises that external directors enhance the ability of an organisation to protect itself against the external environment, reduce uncertainty, or appoint resources that increase the organisation’s ability to raise funds or increase its status and recognition. The influence of the board as a resource is likely to vary between organisations of different sizes. Where size and diversity of boards may be major benefits for small businesses, they may act as constraints for larger organisations.

The counselling and advisory roles of directors are also likely to vary strongly between organisations of different sizes. In small businesses the role of directors’ advice is likely to be more critical and to be based
on closer involvement, personal trust and personal working relations with the CEO or owner/manager.

The third approach which underlines the control role of directors, suggests that as organisation size increases the capacity of the directors to exercise detailed monitoring or evaluation of the CEO and senior managers decreases. In small businesses, the ownership and management interests are often closely coincident because management is focused within a single owner or a small group of owner-managers that act as partners in controlling the firm. There is, therefore, less scope for agency behaviour to develop, and hence a less significant need for additional directors to exercise a control function.

Although corporate governance has traditionally been associated with large organisations only, small businesses can benefit considerably from applying corporate governance principles and the existence of a board of directors. Corporate governance can establish better management practices and performance, and provide easier access to funding. Non-executive directors can assist small businesses in better decision-making and in attracting resources.

3.7 Conclusion

This chapter provided an overview of corporate governance and its implications for small businesses.

Corporate governance is the system by which companies are directed and controlled and consists of a number of systems, processes and practices to ensure that organisations are controlled effectively. It is the responsibility of the boards of directors to ensure that their organisations are well governed.

One of the reasons corporate governance was developed, was because investors were concerned about the excessive concentration of power in the
hands of management. Corporate governance provides better levels of disclosure and offers several other benefits. An organisation can add significant shareowner value by maintaining good corporate governance.

Corporate governance standards differ from one country to the next. Yet, there are certain core elements like fairness, accountability, responsibility and transparency that exist in most standards. Corporate governance in South Africa, the United States and the United Kingdom is addressed by, respectively, the King Report on Corporate Governance, The Sarbanes-Oxley Act of 2002 and the Combined Code.

Although corporate governance has in the past been associated with large organisations only, it is applicable to small businesses and provides them with a number of benefits. These benefits include easier access to funding, better management practices and greater opportunities for growth. The existence of non-executive directors can provide small businesses with a new strategic outlook and help attract better resources.

IT governance is a subset of corporate governance. In the next chapter, IT governance will be addressed and placed in the context of corporate governance. This is necessary in order to appreciate the importance of IT governance in small businesses.
Chapter 4

IT Governance

4.1 Introduction
4.2 What is IT governance?
4.3 Why IT governance?
4.4 Who is responsible for IT governance?
4.5 IT governance frameworks
4.6 Conclusion
4.1 Introduction

In chapter three corporate governance and its implications for small businesses were addressed. It was found that corporate governance is applicable to small businesses and can provide them with a number of benefits. IT governance is a fundamental part of corporate governance. The aim of this chapter is to provide information on IT governance and act as a steppingstone for studying IT governance in small businesses.

IT governance is concerned with the alignment of business and IT goals, and the mitigation of IT risks. IT governance will be discussed by focusing on its purpose and objectives and by looking at the difference between IT governance and IT management.

Organisations can benefit from the successful application of IT governance. The reasons why organisations should apply IT governance and who, in an organisation, is ultimately responsible for IT governance, will be addressed.

Standard IT governance frameworks that have been developed through the combined experience of many individuals are available. By adopting such frameworks to suit their own needs organisations can benefit significantly. Three of the most accepted IT governance frameworks will be discussed in this chapter.

4.2 What is IT governance?

This section will discuss what IT governance is, and point out the difference between IT governance and IT management. The purpose, objectives and focus areas of IT governance will also be addressed.

IT governance is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the
organisation’s IT sustains and extends the organisation’s strategies and objectives (IT Governance Institute, 2003, p. 10).

The difference between IT governance and IT management is often unclear. IT management is focused on the internal effective supply of IT services and products and the management of present IT operations. IT governance, in turn, is much broader, and concentrates on performing and transforming IT to meet present and future demands of the business (internal focus) and the business’s customers (external focus) (Van Grembergen, De Haes & Guldentops, 2004, p. 4). This difference is visually depicted in Figure 4.1.

*Figure 4.1. IT governance and IT management (Van Grembergen et al., 2004).*
The purpose of IT governance is to direct IT endeavours to ensure that IT's performance meets the following objectives (IT Governance Institute, 2003, p. 11):

- Alignment of IT with the enterprise and realisation of the promised benefits.

- Use of IT to enable the enterprise by exploiting opportunities and maximising benefits.

- Responsible use of IT resources.

- Appropriate management of IT-related risks.

Fundamentally, IT governance is concerned with two objectives: IT's delivery of value to the business and the mitigation of IT risks. The first is driven by the strategic alignment of IT with the business. The second is driven by embedding accountability into the enterprise. Both need to be supported by adequate resources and measured to ensure that the results are obtained (IT Governance Institute, 2003, p. 19).

This leads to the five main focus areas for IT governance. Two of these are outcomes: value delivery and risk management. The other three are drivers: strategic alignment, resource management (which overlays them all) and performance measurement (IT Governance Institute, 2003, p. 19).

IT governance is a subset of corporate governance and is concerned with the mitigation of IT risks and aligning the business and IT to create value. It is much broader than IT management, and focuses on the present and future demands of the business and the business's customers. In the next section the reasons why it is necessary to apply effective IT governance will be discussed.
4.3 Why IT governance?

While IT is already critical to enterprise success, provides opportunities to obtain a competitive advantage and offers a means for increasing productivity, it will do all this even more so in the future. An ever-larger percentage of the market value of enterprises has transitioned from the tangible (inventory, facilities, etc.) to the intangible (information, knowledge, expertise, reputation, trust, patents, etc.). Many of these assets revolve around the use of IT (IT Governance Institute, 2003, p. 13). Successful deployment of IT governance creates numerous benefits for business and IT. In this section, these benefits and the reasons why organisations should apply IT governance will be addressed.

Effective IT governance helps ensure that IT supports business goals, maximises IT investment, and appropriately manages IT-related risks. It also helps achieve critical success factors by efficiently and effectively deploying secure, reliable information and applied technology (Callahan, Bastos & Keyes, 2004, p. 346).

An appropriate IT governance programme helps organisations confidently address critical business issues such as the risks of ageing technologies or undertaking e-business. Through IT governance, an enterprise can protect its investment in IT and assure appropriate management of information assets, many of which are vital to the survival and growth of the enterprise itself (Callahan et al., 2004, p. 346).

One of the major reasons IT governance is important is that expectations and reality often do not match (IT Governance Institute, 2003, p. 13). Boards of directors usually expect management to:

- Deliver IT solutions of the right quality, on time and on budget,

- Harness and exploit IT to return business value, and
• Leverage IT to increase efficiency and productivity while managing IT risks.

Ineffective IT governance is likely to be a root cause of the negative experiences many boards of directors have had with IT:

• Business losses, damaged reputations or weakened competitive positions.

• Deadlines that were not met, costs that were higher than expected and quality that was lower than anticipated.

• Enterprise efficiency and core processes that were negatively impacted by the poor quality of IT deliverables.

• Failures of IT initiatives to bring innovation or deliver the promised benefits.

It is clear that the effective implementation of IT governance can offer many benefits for an organisation. IT governance is essential in the alignment of IT with business goals and the management of IT-related risks. It is, therefore, understandable that IT governance is not only the concern of IT management, but also the business. The next section will explore exactly who is responsible for IT governance.

4.4 Who is responsible for IT governance?

This section will look at who is responsible for the implementation of IT governance in an organisation.

IT governance is the responsibility of the board of directors and executive management (IT Governance Institute, 2007, p. 5). IT governance
responsibilities form part of a broad framework of enterprise governance and should be addressed like any other strategic agenda item of the board (IT Governance Institute, 2003, p. 11).

Although they are the responsibility of the board and executive management, governance activities must flow through various levels of the enterprise. Due to complexity and specialisation, the board and executive must set direction and insist on control, while needing to rely on the lower layers in the enterprise to provide the information required in decision-making and evaluation activities. To have effective IT governance in the enterprise, the lower layers need to apply the same principles of setting objectives, providing and getting direction, and providing and evaluating performance measures (IT Governance Institute, 2003, p. 14).

Ultimately, the board of directors and executive management are responsible for the implementation of IT governance. In the next section the IT governance frameworks that are available to assist them with this responsibility will be summarised.

4.5 IT governance frameworks

Organisations can develop their own IT governance frameworks based on the best practice experience found within the organisation, or they can adopt standards that have been developed and near perfected through the combined experience of hundreds of organisations and people. This section will discuss three standard IT governance frameworks and the benefits that an organisation can realise by adopting such a framework.

Spafford (2003) identified a number of reasons to adopt standard IT governance frameworks:

- The Wheel Exists. Time is a precious commodity. It is unnecessary for organisations to spend a lot of time and effort on developing a
framework, based on limited experience, when internationally developed standards already exist.

• Structured. The framework of the models provides an excellent structure that organisations can follow. Furthermore, the structure helps everyone be on the same page because they can see what is expected.

• Best Practices. The standards have been developed over time and assessed by hundreds of people and organisations all over the world. The cumulative years of experience reflected in the models cannot be matched by a single organisation's efforts.

• Knowledge Sharing. By following standards, people can share ideas between organisations. They can also benefit from user groups, websites, magazines, books, etc. Proponents of company-specific, ad hoc approaches do not have this luxury.

• Auditable. Without standards, it becomes far more difficult for auditors, especially third-party auditors, to effectively assess control.

A number of standard IT governance frameworks exist today. Three of the most widely used frameworks are CobiT, the ISO/IEC 27000-series and ITIL. These three frameworks will be discussed in the sub-sections following.

4.5.1 CobiT

This sub-section will address CobiT by reviewing its history and summarising the CobiT products and framework.

The Control Objectives for Information and Related Technology (CobiT) were developed by the Information Systems Audit and Control Foundation (ISACF) in 1996. ISACF later became the Information
Systems Audit and Control Association (ISACA). ISACA is now a
global organisation, with over 50000 members in more than 140
countries. In 1998, ISACA established the IT Governance Institute
(ITGI), which is now responsible for CobiT. During 2007, ITGI released

CobiT is focused on what is required to achieve adequate management
and control of IT, and is positioned at a high level. The more detailed
IT standards and best practices are at a lower level of detail describing
how to manage and control specific aspects of IT. CobiT acts as an
integrator of these different guidance materials, summarising key
objectives under one umbrella framework that also links to governance
and business requirements (IT Governance Institute, 2007, p. 177). For
CobiT 4.1, six of the major global IT-related standards, frameworks
and practices were focused on as the major supporting references to
ensure appropriate coverage, consistency and alignment. These are:

- COSO
  - Internal Control – Integrated Framework, 1994

- Office of Government Commerce (OGC)
  - IT Infrastructure Library (ITIL), 1999-2004

- International Organisation for Standardisation
  - ISO/IEC 27000

- Software Engineering Institute (SEI)
  - SEI Capability Maturity Model (CMM), 1993
  - SEI Capability Maturity Model Integration (CMMI), 2000
The CobiT products have been organised into three levels designed to support executive management and boards, business and IT management, and governance, assurance, control and security professionals. They include (IT Governance Institute, 2007, p. 7):

- **Board Briefing on IT Governance, 2nd Edition.** The briefing helps executives understand why IT governance is important, what its issues are and what their responsibilities are for managing it.

- **Management guidelines/maturity models.** They help assign responsibility, measure performance, and benchmark and address gaps in capability.

- **Frameworks.** Frameworks organise IT governance objectives and good practices by IT domains and processes, and links them to business requirements.

- **Control objectives.** Control objectives provide a complete set of high-level requirements to be considered by management for effective control of each IT process.

- **IT Governance Implementation Guide: Using CobiT and Val IT, 2nd Edition.** The guide provides a generic road map for
implementing IT governance using the CobiT and Val IT resources.

- CobiT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition. Control practices provide guidance on why controls are worth implementing and how to implement them.

- IT Assurance Guide: Using CobiT. Provides guidance on how CobiT can be used to support a variety of assurance activities together with suggested testing steps for all the IT processes and control objectives.

The CobiT framework was created with the main characteristics of being business-focused, process-oriented, controls-based and measurement-driven (IT Governance Institute, 2007, p. 10).

**Business-focused**

Business orientation is the main theme of CobiT. It is designed not only to be employed by IT service providers, users and auditors, but also, and more importantly, to provide comprehensive guidance for management and business-process owners.

The CobiT framework is based on the following principle (Figure 4.2): to provide the information that the enterprise requires to achieve its objectives, the enterprise needs to invest in and manage and control IT resources, using a structured set of processes to provide the services that deliver the required enterprise information.

Managing and controlling information is at the heart of the CobiT framework and help ensure alignment to business requirements. To satisfy business objectives, information needs to conform to certain
control criteria, which CobiT refers to as business requirements for information. The seven distinct, certainly overlapping, information criteria are effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability.

To respond to the business requirements for IT, the enterprise needs to invest in the resources required to create an adequate technical capability to support a business capability resulting in the desired outcome. The IT resources identified in CobiT are applications, information, infrastructure and people.

**Process-oriented**

CobiT defines IT activities in a generic process model within four domains. These domains are:

1. Plan and Organise (PO). This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives.
2. Acquire and Implement (AI). To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure the solutions continue to meet business objectives.

3. Deliver and Support (DS). This domain is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and operational facilities.

4. Monitor and Evaluate (ME). All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses performance management, monitoring of internal control, regulatory compliance and governance.

Across these four domains, CobiT has identified 34 IT processes that are generally used. While most enterprises have defined plan, build, run and monitor responsibilities for IT, and most have the same key processes, few will have the same process structure or apply all 34 CobiT processes. CobiT provides a complete list of processes that can be used to verify the completeness of activities and responsibilities. However, they need not all apply, and, even more, they can be combined as required by each enterprise.

For each of these 34 processes, a link is made to the business and IT goals that are supported. Information on how the goals can be measured, what the key activities and major deliverables are, and who is responsible for them is also provided.
**Controls-based**

CobiT defines control objectives for all 34 processes, as well as overarching process and application controls. Control is defined as the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented, or detected and corrected. IT control objectives provide a complete set of high-level requirements to be considered by management for effective control of each IT process.

**Measurement-driven**

A basic need for every enterprise is to understand the status of its own IT systems and to decide what level of management and control the enterprise should provide. Obtaining an objective view of an enterprise’s own performance level is not easy. Enterprises need to measure where they are and where improvement is required, and implement a management tool kit to monitor this improvement.

CobiT deals with these issues by providing:

- Maturity models to enable benchmarking and identification of necessary capability improvements.

- Performance goals and metrics for the IT processes, demonstrating how processes meet business and IT goals and are used for measuring internal process performance based on balanced scorecard principles.

- Activity goals for enabling effective process performance.
Figure 4.3. The CobiT framework (IT Governance Institute, 2007).
The overall CobiT framework can be shown graphically, as depicted in Figure 4.2, with the process model of four domains containing 34 generic processes, managing the IT resources to deliver information to the business according to business and governance requirements.

This sub-section summarised the CobiT framework and products. CobiT is focused on what is required to achieve IT governance, and is positioned at a high level. The ISO/IEC 27000-series of standards, summarised in the next sub-section, are at a lower level of detail.

4.5.2 The ISO/IEC 27000-series

The ISO/IEC 27000-series is comprised of information security standards published jointly by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC). At present, three of the standards in the series are publicly available, while several more are under development (ISO 27000 Directory, 2008). Two of the published standards, ISO/IEC 27002 and ISO/IEC 27001, will be discussed further.

ISO/IEC 27002

ISO/IEC 27002 provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining information security management systems (ISMS) (ISO 27000 Directory, 2008).

After the introductory sections, the standard contains the following 12 main sections (ISO/IEC, 2005):

1. Risk assessment and treatment,
2. Security policy,
3. Organisation of information security,
4. Asset management,
5. Human resources security,
6. Physical and environmental security,
7. Communications and operations management,
8. Access control,
9. Information systems acquisition, development and maintenance,
10. Information security incident management,
11. Business continuity, and
12. Compliance.

ISO/IEC 27001


It is intended to be used in conjunction with ISO/IEC 27002 and is the certification standard against which organisations’ ISMSs may be certified. Organisations that implement an ISMS in accordance with
the best practice advice in ISO/IEC 27002 are likely to simultaneously meet the requirements of ISO/IEC 27001, but certification is entirely optional (ISO 27000 Directory, 2008).

ISO/IEC 27001 certification usually involves a three-stage audit process (ISO 27000 Directory, 2008):

1. Stage 1 is a "table top" review of the existence and completeness of key documentation such as the organisation's security policy, Statement of Applicability (SoA) and Risk Treatment Plan (RTP).

2. Stage 2 is a detailed, in-depth audit involving testing the existence and effectiveness of the information security controls stated in the SoA and RTP, as well as their supporting documentation.

3. Stage 3 is a follow-up reassessment audit to confirm that a previously-certified organisation remains in compliance with the standard. Certification maintenance involves periodic reviews and re-assessments to confirm that the ISMS continues to operate as specified and intended.

The ISO/IEC 27000-series comprises information security standards. ISO/IEC 27002 provides best practice recommendations on information security management, while ISO/IEC 27001 is the certification standard against which organisations may be certified. The next subsection will summarise ITIL, which focuses more on service management.
4.5.3 ITIL

The IT Infrastructure Library (ITIL) was created by the British Office of Government Commerce (OGC) to more effectively manage IT within British authorities as well as public companies. The principles of the ITIL framework were derived from best practice with regards to observed companies within the IT sector. It is now a fully documented set of best practice documents for IT service management and the most widely accepted approach to IT service management in the world (APM Group, 2008). It consists of several books, hence the term, library. At the moment, there are nine core publications (APM Group, 2008):

1. Service Support,
2. Service Delivery,
3. Planning to Implement Service Management,
4. Application Management,
5. ICT Infrastructure Management,
6. Security Management,
7. Software Asset Management,
8. The Business Perspective, Volume 1: The IS View on Delivering Services to the Business, and

ITIL’s main objectives are to provide best practice definitions and criteria for operations management within two key areas: Service Support and Service Delivery. In these areas, ITIL focuses on the operational, organisational and functional attributes required for optimised operations management. These areas also have a number of supporting subcategories. ITIL, however, does not cover the strategic impact of IT and the relation between IT and the business (Etzler, 2007, p. 20).
ITIL is a set of best practices for IT service management, and aims to provide best practice definitions and criteria for operations management within service support and service delivery.

Organisations can benefit considerably from using standard frameworks to implement IT governance. These standards reflect the best practice experience of many individuals and organisations and allow organisations to save time and share knowledge with other organisations.

A number of standard IT governance frameworks exist, each providing a different perspective on IT governance. CobiT is business-focused, process-oriented and controls-based, and focuses on what is required from an IT governance perspective. The ISO/IEC 27000-series of standards provide a lower level of detail and comprises information security standards addressing the how from a security perspective. ITIL, on the other hand, focuses on IT service management, and provides guidelines for service support and delivery.

4.6 Conclusion

IT governance is an integral part of enterprise governance and is concerned with IT's delivery of value to the business and the mitigation of IT risks. Apart from value delivery and risk management, IT governance also focuses on strategic alignment, resource management and performance management.

The successful implementation of IT governance can hold many benefits for organisations. It plays an important role in ensuring that organisations can successfully manage and control IT activities and infrastructure, and can assist organisations in bridging the gap between business and IT.

IT governance is the responsibility of the board of directors and executive management and should be addressed like any other strategic agenda item of the board.
There are many standard IT governance frameworks available that organisations can utilise to implement IT governance. Three of the most widely used frameworks are CobiT, the ISO/IEC 27000-series and ITIL. These best practices have been developed by many industry experts and can help organisations save time in implementing IT governance.

In the previous chapter, the implications of corporate governance for small businesses were discussed. Like corporate governance, IT governance can easily be perceived as being only applicable to large organisations. In the next chapter IT governance will be discussed in the context of small businesses.
Chapter 5

IT Governance in Small Businesses

5.1 Introduction
5.2 IT in small businesses
5.3 IT governance in small businesses
5.4 Characteristics of IT governance in small businesses
5.5 Conclusion
5.1 Introduction

The previous chapter discussed IT governance by looking, amongst others, at what it entails and the benefits it can provide an organisation. Three of the best-known standard IT governance frameworks were also addressed.

IT governance is often perceived as only being relevant to large organisations. In this chapter, IT governance in the context of small businesses will be addressed. The purpose of the chapter is assess whether IT governance is applicable to small businesses as well and, if so, how it differs for small businesses.

Before addressing IT governance, it will be of value to look at information technology and the role it plays in small businesses. The IT risks and problems facing small businesses and the effect of information security on small businesses will be discussed.

The chapter will conclude by presenting seven characteristics of IT governance in small businesses. These characteristics will lead to certain requirements that an IT governance framework for small businesses should conform to.

5.2 IT in small businesses

IT functions in small businesses differ from those in larger organisations. The IT functions in small businesses tend to have a more centralised structure with the CEO or business owner. Small businesses also, generally, have difficulty in attracting and retaining skilled IT staff, and, therefore, have smaller or no IT departments and a lack of IT specialists. This is mostly due to the lack of resources that can be associated with small businesses (Yang & Jing, 2008, p. 326).
This section will address IT in small businesses by focusing on their dependence on external advice, the factors that influence IT adoption in small businesses, the problems and risks they face, and the importance of information security in small businesses.

5.2.1 External advice

Due to the smaller or non-existent IT departments of small businesses, business owners are typically at the head of the IT department (Geiger & Wegman, 2002) and have to do a great deal of the IT-related work themselves. Because of this, and the limited resources available to small businesses, they must often rely on outsourcing and external consultants for service and support (Yang & Jing, 2008, p. 326).

In a study by Burke and Jarratt (2004, p. 132), it was found that limited resources (including managers’ time) or capabilities within the businesses are definite incentives to outsource for advice. Limited time, though, can be both a constraint and a driver for seeking outside advice. Respondents agree that advice needs to be practical, and they calculate the value of advice by comparing the cost of obtaining it with the expected benefit that it will bring. Some are simply not prepared to pay for information.

Small businesses must exercise caution when using external consultants, as that they may not always be trustworthy and reputable (Gupta & Hammond, 2005, p. 308). Instability in service providers and a lack of outsourcing service level agreements can put small businesses at risk (Upfold & Sewry, 2005, p. 3).

Due to a lack of resources and IT specialists, small businesses often have to seek external advice for IT-related matters. These factors also influence the adoption of IT in an organisation. This aspect will be addressed in the next sub-section.
5.2.2 IT adoption

As a result of business size and economic characteristics, IT adoption in small businesses differs from that in large organisations (Yang & Jing, 2008, p. 326). There are several factors that influence IT adoption in small businesses. Two of the most significant factors are available resources and the outlook of the CEO or owner:

- **Resources.** Because of size and resource limitations, small businesses do not normally have formal IT departments and depend more on external support and service (Yang & Jing, 2008, p. 326).

- **CEO or owner.** Small businesses tend to have a more centralised structure and more informal decision making. The decision behaviour of the top manager usually represents the decision behaviour of the whole business (Yang & Jing, 2008, p. 326). Businesses with CEOs who are more knowledgeable about IT are more likely to adopt IT (Thong & Yap, 1995, p. 432).

The availability of resources in a small business and the IT knowledge of the CEO or owner play a big part in the business’s adoption of IT. In the next sub-section the IT problems that face small businesses will be discussed.

5.2.3 IT problems and risks facing small businesses

Some of the problems facing small businesses that have already been discussed are a lack of resources and limited technical skills. This sub-section will address the more direct risks and problems that small businesses may encounter.
According to industry analysts (Colby, 2004), the biggest problem that faces small businesses with regard to information technology is, without a doubt, security. For example, consider industry magazine Information Week's 2002 Global Information Security Survey. The survey polled small businesses for 12 months (through the third quarter 2002), with the following results:

- 41 percent experienced a loss of network availability as a result of a security incident.
- 41 percent had either a virus, worm or Trojan horse attack.
- 19 percent had security breaches resulting in more than 24 hours of downtime.

Some of the current security threats facing small businesses are security holes or vulnerabilities, direct attacks, viruses, worms, Trojan horses, denial of service attacks, spam and spyware (Nijnik, 2005). Information security will be discussed in more detail in the next sub-section.

### 5.2.4 Information security in small businesses

In this sub-section, information security in small businesses and the key aspects of security management will be addressed.

Small businesses are more vulnerable to security attacks because they lack the financial resources and expertise required to develop a comprehensive information security system (Gupta & Hammond, 2005, p. 298). Small business owners may also be too busy with running the business to formulate an information security strategy (Gupta & Hammond, 2005, p. 307).
Surveys show that in Australia, 45 percent of firms do not budget for computer security (Gupta & Hammond, 2005, p. 300). In the UK, 49 percent of firms list budget constraints as the primary issue in implementing computer security (Gupta & Hammond, 2005, p. 300).

The challenge of creating and implementing a security strategy, and the extent of the task, results in many small businesses feeling tempted to “cut corners”. However, knowing where to take shortcuts and where not to, can mean the difference between security success and disaster (Gupta & Hammond, 2005, p. 299).

Some of the key aspects of security management include:

- **Information security policies.** Small businesses are less likely to have a written security policy than larger organisations. This may be due to lack of financial resources or technical expertise, or simply because owners are too busy to formulate an information security strategy. In the UK, 42 percent of firms do not have information security policies (Gupta & Hammond, 2005, p. 300).

- **Training and awareness.** Inadvertent information security threats pose a high risk to small businesses, and yet training and awareness programs are often neglected (Upfold & Sewry, 2005, p. 3). The appropriate training and awareness within the organisation to promote a security culture is needed (Gupta & Hammond, 2005, p. 300).

- **Backups and disaster recovery.** In a 2004 survey (Upfold & Sewry, 2005, p. 2), it was found that up to 25 percent of small businesses do not have formal data backup and storage facilities, and 26 percent are not confident that they can restore files after an incident. This is alarming given that in the same
survey, two thirds of respondents indicated that they had an information security incident in that year.

- Anti-virus protection. In the above mentioned survey, viruses caused the greatest number of serious incidents. Regular anti-virus updates and operating system updates are vital for staying protected against viruses, Trojan horses, spyware, etc.

Small businesses are more vulnerable to security attacks, and tend not to implement security management aspects like information security policies, training and awareness, backups and disaster recovery, and anti-virus protection.

The IT departments in small businesses differ considerably from those in larger organisations. Small businesses have a lack of resources and IT specialists, and have to rely on external consultants for advice and support. The adoption of IT in small businesses is also affected by these factors and the IT knowledge of the CEO or business owner.

Small businesses face many IT-related risks and problems. The biggest problem they face is security related threats like viruses and spyware. Because small businesses might be more vulnerable to security threats, it is important that they apply good information security management techniques.

The characteristics of IT in small businesses, and the problems they face, influence the role that IT governance can perform and the way it should be implemented in small businesses. These issues will be addressed in the next section.

5.3 IT governance in small businesses

This section will address the implementation of IT governance in small businesses. The benefits and constraints of implementing IT governance in
small businesses and the applicability of standard IT governance frameworks to small businesses will be discussed.

As stated before, IT governance is often perceived as only relevant to large organisations. It is, however, a key element of any organisation. As discussed in chapter four, IT governance is about applying IT in such a way that it creates value for the business, while balancing the risk versus return. Small businesses also want to create value by applying IT. This, together with the fact that corporate governance, of which IT governance is a subset, applies to small businesses, makes IT governance completely applicable to small businesses.

Many authors agree (Moir, 2006; De Graaf, 2008) that IT governance is necessary for small businesses as well, and not implementing it can threaten the short and long term business value, or even the short-term survival of the business.

Existing frameworks like CobiT are too extensive for small businesses to use in implementing IT governance (De Graaf, 2008). They are too complex and costly to implement and small businesses may consider the process intimidating and unachievable (Upfold & Sewry, 2005, p. 5). Small businesses should convert the high-level concept of governance into practical and easy to implement best practices (De Graaf, 2008).

In 2006, ISACA conducted a study (Armstrong, 2008) to determine the top CobiT controls that SMEs should have in place for securing information assets. These controls turned out to be network security, virus protection, backups, file access privilege controls, IT as part of strategic plans, IT continuity and recovery plans, ID and authorisation procedures, management support/buy-in, risk evaluation programme, employee IT security training and data input controls. Table 5.1 lists the ten controls with the technologies or procedures that must be implemented to create the controls.
<table>
<thead>
<tr>
<th>Rank</th>
<th>Control Objective</th>
<th>What to Implement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Network security</td>
<td>Updated firewall, secure wireless transmissions</td>
</tr>
<tr>
<td>2.</td>
<td>Virus protection</td>
<td>Updated anti-virus, anti-spyware applications</td>
</tr>
<tr>
<td>3.</td>
<td>Backups</td>
<td>Regular and tested backup procedures</td>
</tr>
<tr>
<td>4.</td>
<td>File access privilege controls</td>
<td>Role-based access control, least privilege</td>
</tr>
<tr>
<td>5.</td>
<td>IT as part of strategic plans</td>
<td>Technologies that support business goals</td>
</tr>
<tr>
<td>6.</td>
<td>IT continuity and recovery plan</td>
<td>Basic disaster recovery plan (DRP) procedures</td>
</tr>
<tr>
<td>7.</td>
<td>ID and authorisation procedures</td>
<td>Complex passwords, password change policies</td>
</tr>
<tr>
<td>8.</td>
<td>Management support/buy-in</td>
<td>Leadership from CEO for IT control projects</td>
</tr>
<tr>
<td>9.</td>
<td>Risk evaluation programme</td>
<td>Basic risk assessment and/or self-audits</td>
</tr>
<tr>
<td>10.</td>
<td>Employee IT security training</td>
<td>Training for e-mail, Web, and password use</td>
</tr>
<tr>
<td>11.</td>
<td>Data input controls</td>
<td>Field formats, periodic data range testing</td>
</tr>
</tbody>
</table>

*Table 5.1. Controls that SMEs should have in place for securing information assets (Armstrong, 2008).*
Small businesses should not waste time with unnecessary paperwork and unproductive meetings (De Graaf, 2008), and can make use of readily available tools such as spreadsheets and e-mail to avoid the licensing and support costs that come with the solutions designed for large organisations (Moir, 2006).

Another constraint facing small businesses in implementing IT governance is the lack of IT staff. A small business with limited staff resources is going to need a consultant to help implement IT governance controls (Armstrong, 2008). Organisations implementing IT governance frameworks spend a lot of money on implementing and hiring consultants (IT Business Edge, 2006). But, as discussed earlier, financial constraints are a problem for small businesses and they may not be able to afford hiring consultants to implement IT governance.

Although most of the existing standard IT governance frameworks are too extensive for small businesses to use as is, some of them do contain sections or simpler versions that are applicable to small and medium-sized enterprises. Examples are CobiT QuickStart, a separate publication by ISACA, and the Information security starting point that forms part of ISO/IEC 27002. These two examples will be addressed in the following subsections.

5.3.1 CobiT QuickStart

CobiT QuickStart, now in its second version, is a baseline for small and medium-sized enterprises and other organisations where IT is not mission-critical or essential for survival. It can also serve as a starting point for organisations in their move towards an appropriate level of control and IT governance (IT Governance Institute, 2007b, p. 6).

CobiT QuickStart 2.0 is based on a selection of the processes and control objectives of CobiT 4.1. Where CobiT consists of 210 control
objectives and 34 processes in four domains, QuickStart consists of 59 control objectives and 32 processes in four domains (IT Governance Institute, 2007b, p. 14).

CobiT QuickStart consists of a framework and a baseline. The framework describes what QuickStart is, why it is needed and how to determine its suitability for a given organisation. The baseline consists of the processes and control objectives, as well as simplified versions of Responsible, Accountable, Consulted and Informed (RACI) charts and key metrics (IT Governance Institute, 2007b).

CobiT QuickStart is a simplified version of CobiT aimed at small and medium-sized enterprises, and can be used as a starting point for organisations in their move towards implementing CobiT.

5.3.2 ISO/IEC 27002’s Information security starting point

ISO/IEC 27002 contains a section named Information security starting point which highlights certain controls that are applicable to most organisations and in most environments (ISO/IEC, 2005, p. x).

The controls considered to be common best practice for information security include:

- Information security policy document,
- Allocation of information security responsibilities,
- Information security awareness, education and training,
- Correct processing in applications,
- Technical vulnerability management,
- Business continuity management, and
- Management of information security incidents and improvements.
The controls considered to be essential to an organisation from a legislative point of view include:

- Data protection and privacy of personal information,
- Protection of organisational records, and
- Intellectual property rights.

The Information security starting point lists information security controls that apply to most organisations and in most environments.

IT governance is applicable to small businesses and can assist them in creating value and managing risk. The problem for small businesses, though, is that their lack of resources renders existing standard frameworks too extensive and resource intensive for them to implement. Small businesses should use easy to implement best practices and make use of readily available tools such as spreadsheets and e-mail.

By studying the various aspects of IT and IT governance in small businesses and comparing those to larger organisations, it is clear that there are many differences between small businesses and larger organisations. In the next section, seven characteristics that distinguish IT governance in small businesses will be derived.

### 5.4 Characteristics of IT governance in small businesses

The implementation of IT governance in small businesses and larger organisations differ considerably. In this section, seven characteristics that make IT governance in small businesses unique will be proposed. The characteristics were derived by addressing the risks facing small businesses, and looking at other factors that distinguish IT and IT governance in small businesses from large organisations.
An IT governance framework aimed at small businesses will have to address and comply with these seven characteristics to effectively support the implementation of IT governance.

5.4.1 No boards of directors

In chapter three, it was conclusively stated that corporate governance is the responsibility of an organisation’s board of directors. IT governance is a subset of corporate governance and is, therefore, also the responsibility of the board. This was reiterated in chapter four when the responsibility for IT governance was discussed.

Small businesses, however, do not always have a board of directors, as was discussed in chapter three. If a business does not have a board, the responsibility for IT governance will lie with the CEO or owner of the business. Small businesses have a more centralised structure and the decision behaviour of the top manager usually represents the decision behaviour of the whole business (Yang & Jing, 2008, p. 326). The CEO or owner plays an important role in the adoption of IT. Businesses with CEOs who are more knowledgeable about IT are more likely to adopt IT (Thong & Yap, 1995, p. 432).

An IT governance framework for small businesses will have to make provision for businesses without boards of directors or similar structures.

5.4.2 Limited management structures

Small businesses do not have the extensive management structures of larger organisations. In chapter two, the different forms of ownership and management models applicable to small businesses were discussed. Ownership of large organisations is normally distanced from
management, which is not the case in the majority of small businesses (Beaver & Prince, 2004, p. 35).

Many small businesses do not have a CIO that can act as an internal sponsor and guide the implementation of IT governance controls. However, many small businesses have a financial manager or manager with deep accounting experience. According to Armstrong (2008), IT must look to this individual to obtain advice for strategic direction.

An IT governance framework for small businesses must make provisions for businesses with limited management structures.

5.4.3 Small or non-existent IT departments

Section 5.2 discussed the characteristics of IT in small businesses. It was stated that small businesses, typically, have small or no IT departments, and a lack of IT specialists (Yang & Jing, 2008, p. 326). The implementation of IT governance might, therefore, be the responsibility of non-IT staff or IT staff that do not specialise in IT governance.

An IT governance framework for small businesses should not contain IT jargon and must be simple enough to be understood by non-IT staff or IT staff that do not specialise in IT governance.

5.4.4 Lack of resources

Some of the problems facing small businesses that were addressed throughout this chapter are a lack of financing and technical expertise.

Small businesses suffer from a condition commonly referred to as resource poverty. Resource poverty results from conditions that are unique to small businesses, such as operating in a highly competitive
environment, financial constraints and a lack of professional expertise. Because of these conditions, small businesses are characterised by severe constraints on financial resources and a lack of in-house IT expertise (Thong & Yap, 1995, p. 432). Time is also a problem as the owner and managers are normally busy with other business priorities (Gupta & Hammond, 2005, p. 300).

Small businesses need an IT governance framework that is less time-consuming, costs less to implement and can be implemented by fewer employees.

5.4.5 Less complex frameworks

As discussed in section 5.3, existing IT governance frameworks are complex and aimed at large organisations. These frameworks can be too overwhelming and challenging for small businesses to implement.

Small businesses need an IT governance framework that is simpler and easier to implement, and only contain controls that are applicable to small businesses.

5.4.6 Focus on information security

As discussed in section 5.2, information security is the biggest IT problem facing small businesses. Many small businesses experience security incidents and breaches due to a lack of or ineffective security systems.

They, typically, do not possess some of the basic elements of security management like information security policies, backup and disaster recovery, security awareness and up-to-date anti-virus protection.
An IT governance framework aimed at small businesses will have to include a strong emphasis on information security and address the common security risks affecting small businesses.

5.4.7 Low-cost systems

Large organisations make use of expensive applications and support systems to assist in implementing IT governance (IT Business Edge, 2006). Because of the lack of financial and technical resources, small businesses cannot make use of these systems.

Small businesses should be able to implement an IT governance framework using general end-user software packages such as spreadsheets, word processors and e-mail.

An IT governance framework intended for small businesses should take the distinct characteristics of small businesses into account.

The internal structure of small businesses differs from that of large organisations. Small businesses often do not have boards of directors. They have limited management structures and the IT departments are either small or non-existent.

Small businesses suffer from a lack of resources and require a framework that is cost-effective and less time-consuming to implement. The framework should be simple and easy to implement, and have a clear focus on information security.

5.5 Conclusion

This chapter addressed IT and IT governance in the context of small businesses.
IT in small businesses differs from that in larger organisations. Small businesses generally have smaller or no IT departments and a lack of IT specialists. Because of this, non-IT staff has to perform many IT-related activities and the business often relies on external consultants for advice and support.

Small businesses encounter many IT-related problems and risks, of which the biggest is security. Small businesses are more vulnerable to security attacks and should address information security by implementing information security policies, anti-virus protection, and other information security controls.

IT governance is not only applicable to large organisations, but to small businesses as well. However, because of certain factors unique to small businesses, IT governance in the context of small businesses differs quite considerably from that in large organisations. This chapter presented seven characteristics that distinguish IT governance in small businesses to that of large organisations.

Small businesses often do not have boards of directors, they have limited management structures, and they lack IT specialists to implement IT governance. Because of their lack of resources, small businesses require an IT governance framework that is cost-effective and easy to implement. Furthermore, the framework must have a strong focus on information security to address the security issues facing small businesses.

In the next chapter, a framework for IT governance in small businesses will be proposed to address these characteristics and requirements.
Chapter 6

The ITGovSB Framework

6.1 Introduction

6.2 Why a framework for small businesses is needed

6.3 ITGovSB and what it involves

6.4 The ITGovSB framework

6.5 Evaluating ITGovSB against the characteristics of IT governance in small businesses

6.6 Conclusion
6.1 Introduction

In chapter five, IT governance in small businesses was addressed. It was concluded that although IT governance is relevant to small businesses as well, it differs quite significantly to that in large organisations. The objective of this chapter is to propose a framework that can be used to implement IT governance in small businesses.

The chapter will commence by addressing the reasons why small businesses need an IT governance framework that is specifically adapted for small businesses. The characteristics of IT governance in small businesses will be reviewed.

After introducing the framework for IT Governance in Small Businesses (ITGovSB), the structure of the framework and what it involves will be addressed.

Once ITGovSB has been presented, the chapter will conclude by evaluating whether the framework effectively addressed IT governance in small businesses, according to the characteristics developed in the previous chapter.

6.2 Why a framework for small businesses is needed

This section will explore the reasons why small businesses need a framework for IT governance that is designed exclusively for small businesses.

IT governance in small businesses differs from larger organisations. In the previous chapter, seven characteristics of IT governance in small businesses were addressed. These characteristics are:

1. No boards of directors,
2. Limited management structures,
3. Small or non-existent IT departments,
Lack of resources,
5. Less complex frameworks,
6. Focus on information security, and
7. Low-cost systems.

As discussed in the previous chapter, existing IT governance frameworks like CobiT might be too extensive and complex for small businesses to use, as they require a great deal of resources to implement. Small businesses need a framework that is designed specifically for small businesses and conforms to the seven characteristics of IT governance in small businesses.

In this chapter, such a framework, ITGovSB, will be proposed to address IT governance in small businesses. The next section will look at what ITGovSB involves.

6.3 ITGovSB and what it involves

This section will discuss the domains, processes, control objectives and controls that ITGovSB consists of.

The ITGovSB framework is based on the CobiT framework and the ISO/IEC 27002 information security controls. It consists of four domains, nine processes, 27 control objectives and 32 information security controls.

The four domains are Plan and organise, Acquire and implement, Deliver and support, and Monitor and evaluate. These domains are taken from CobiT and maps to IT’s traditional responsibility areas of plan, build, run and monitor (IT Governance Institute, 2007, p. 12).

The general principle that was followed to identify the processes and control objectives was to eliminate processes and control objectives from CobiT as far as possible. Following this process, an attempt was made to combine the remaining processes and control objectives to eventually constitute ITGovSB.
Special focus was given to the control objectives identified by the ISACA survey that was addressed in chapter five (Armstrong, 2008). Where CobiT consists of 34 processes and 210 control objectives, ITGovSB consists of nine processes and 27 control objectives. Thus, it is clear that ITGovSB is less extensive than CobiT.

The CobiT control objectives provide high-level requirements for the control of IT processes (IT Governance Institute, 2007, p. 13). One of the advantages of using CobiT is that it positions information security governance within a wider information technology governance framework. The downside, however, is that although the information security governance component provides good guidance on the “what” that needs to be done, it is not very detailed as far as the “how” it needs to be done is concerned (Von Solms, 2005, p. 101). To provide a more complete or all-inclusive framework to small businesses, it is important to address this practical side of governance as well.

This is where the information security controls of ISO/IEC 27002 can play a role. ISO/IEC 27002 is much more detailed and provides more direct guidelines on how things need to be done from a security perspective. It is, however, a stand alone information security framework, and does not provide the wider platform provided by CobiT. By using both frameworks together, it is possible to get the benefits of both the wider reference and integrated platform provided by CobiT, and the more detailed guidelines provided by ISO/IEC 27002 (Von Solms, 2005, p. 101). This, together with the need to address the security issues facing small businesses, makes the ISO/IEC 27002 information security controls a good choice to complement the CobiT control objectives and to provide a more complete or all-inclusive framework for small businesses. Again, in selecting the information security controls, special focus was given to the controls identified by ISO/IEC 27002’s Information security starting point that was addressed in chapter five.

The ITGovSB framework is based on the CobiT framework and the ISO/IEC 27002 information security controls. The CobiT control objectives provide
high-level requirements for the control of IT processes, while ISO/IEC 27002 is much more detailed and provides more direct guidelines on how the security objectives can be implemented. The ITGovSB framework will be presented in the next section.

6.4 The ITGovSB framework

This section contains the ITGovSB framework. A graphic illustration of the domains and processes of the framework is shown in Figure 6.1.

The CobiT control objectives and ISO/IEC 27002 controls that are referenced in the ITGovSB framework are indicated in parentheses next to the appropriate headings in the framework. A more detailed listing of these control objectives and controls are provided in Appendix A.

Figure 6.1. The ITGovSB domains and processes.
**Domain 1 – Plan and Organise**

This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. A proper organisation as well as technological infrastructure should be put in place.

**Process 1.1 – Plan IT**

This process addresses the higher level management aspects of IT such as strategic planning, general IT planning and IT governance. IT strategic planning and governance manages and directs all IT resources in line with the business strategy to ensure that optimal value is realised from IT investments. Planning is necessary to determine the technological direction to support the business and manage clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms. Planning is also necessary to identify IT risks.

**Control Objectives**

**Define an IT Strategy (PO1.1 – PO1.6)**

Create a strategic IT plan that defines how IT goals will contribute to the business’s strategic objectives and ensure that IT investments have solid business cases. Create tactical IT plans that are derived from the IT strategy and actively manage the IT investments required to achieve specific strategic business objectives.

**IT Planning (PO2.1 – PO2.4, PO3.1 – PO3.5, PO9.1 – PO9.6)**

Analyse existing and emerging technologies, and plan which technological direction is appropriate to realise the IT strategy and the business systems architecture. Also identify which technologies have the potential to create
business opportunities and monitor the business sector, industry, technology, infrastructure, legal and regulatory environment trends. Identify IT risks and assess the likelihood and impact of all identified risks.

Provide IT Governance (ME4.1 – ME4.7)

Define, establish and align the IT governance framework with the overall enterprise governance and control environment. Enable understanding of strategic IT issues and define the enterprise’s appetite for IT risk.

Process 1.2 – Organise and Manage IT

This process addresses the management of the IT department and IT activities. Management defines and communicates IT policies, which ensures awareness and understanding of business and IT risks. An IT organisation is defined by considering requirements for staff, skills, and roles and responsibilities. Other management activities include IT budgets, human resources and projects.

Control Objectives

Manage the IT Department and HR (PO4.1 – PO4.15, PO7.1 – PO7.8, PO8.1 – PO8.6, DS13.1 – DS13.2, DS13.4)

Establish an IT structure (staffing requirements and sourcing solutions) that reflects the business needs. Establish roles and responsibilities for IT personnel and minimise reliance on a single individual performing a critical job function through knowledge capture and sharing. Maintain IT personnel recruitment processes in line with the overall organisation’s personnel policies and procedures.
MANAGE THE IT BUDGET (PO5.1 – PO5.5, DS6.1 – DS6.4)

Prioritise the allocation of IT resources. Prepare an IT budget reflecting the priorities established and the ongoing costs of operating and maintaining the current infrastructure. Compare actual costs to budgets.

MANAGE IT PROJECTS (DS10.1 – DS10.14)

Establish and maintain a project management approach that is applied to IT projects. Obtain commitment and participation from the affected stakeholders in the definition and execution of the project.

COMMUNICATE MANAGEMENT SUPPORT AND POLICIES (PO6.1 – PO6.5)

Develop and maintain IT policies, including an information security policy document, and roll out and enforce IT policies to all relevant staff.

INFORMATION SECURITY CONTROLS

ALLOCATION OF INFORMATION SECURITY RESPONSIBILITIES (6.1.3, 8.1.1)

All information security roles and responsibilities of employees, contractors and third party users should be clearly defined.

SCREENINGS (8.1.2)

Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics. Verification checks should include character references, a check of the applicant’s CV for accurateness, and more detailed checks such as checks for criminal records.
DOCUMENTING OPERATING PROCEDURES (10.1.1)

Operating procedures should be documented, maintained, and made available to all users who need them. Documented procedures should be prepared for system activities such as backups and equipment maintenance.

INFORMATION SECURITY POLICY DOCUMENT (5.1.1, 5.1.2, 6.1.1)

An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties. The policy should be reviewed at planned intervals or if significant changes occur. The document should contain statements concerning:

- A definition of information security.
- A statement of management intent.
- A brief explanation of security policies, principles, standards, and compliance requirements of particular importance to the organisation, including:
  1) compliance with legislative, regulatory, and contractual requirements,
  2) security education, training, and awareness requirements,
  3) business continuity management, and
  4) consequences of information security policy violations.
- A definition of general and specific responsibilities for information security management.

ACCESS CONTROL POLICY (11.1.1)

An access control policy should be established, documented and reviewed regularly. Access control rules and rights should be stated in the policy. The policy should take account of the following:

- Requirements for formal authorisation of access requests.
• Requirements for periodic review of access controls.
• Removal of access rights.

**Domain 2 – Acquire and Implement**

To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented. In addition, changes in and maintenance of existing systems are covered by this domain to make sure the solutions continue to meet business objectives.

**Process 2.1 – Acquire IT Solutions**

This process covers the acquisition of IT solutions. An initial analysis is done to identify solutions and a decision is made to ‘make’ or ‘buy’. Application software is acquired or developed, and the necessary technology infrastructure to support application software (hardware, networking, operating systems, etc.) is acquired. This process also addresses the actual procurement of IT resources (people, hardware, software and services).

**Control Objectives**

**Identify IT Solutions (AI1.1 – AI1.4)**

Identify, prioritise, and agree on business functional and technical requirements needed to achieve the expected outcomes and identify associated risks. Develop a feasibility study that examines the possibility of implementing the requirements.

**Acquire Application Software (AI2.1 – AI2.4, AI2.7 – AI2.9)**

Translate business requirements into a high-level design specification for software acquisition and prepare detailed design and technical software
application requirements. Implement business controls, where appropriate, into application controls so that processing is accurate, complete, timely, authorised and auditable. Ensure that all legal and contractual aspects are identified and addressed for application software developed by third parties.

ACQUIRE TECHNOLOGICAL INFRASTRUCTURE (AI3.1)

Provide a reliable and secure IT infrastructure and appropriate platforms for the business applications in line with the defined IT architecture and technology standards and the organisation’s technological direction.

PROCURE IT SOLUTIONS (AI5.1 – AI5.4)

Follow a set of procedures and standards that is consistent with the business’s overall procurement process to acquire IT resources needed by the business. Select suppliers according to a fair and formal practice to ensure a viable best fit based on specified requirements. Requirements should be optimised with input from potential suppliers.

INFORMATION SECURITY CONTROLS

SECURITY REQUIREMENTS ANALYSIS (12.1.1)

Statements of business requirements for new information systems, or enhancement to existing information systems should specify the requirements for security controls. Specifications should consider automated controls to be incorporated in the information systems, and the need for supporting manual controls. Similar consideration should be applied when evaluating software packages, developed or purchased, for business applications.
Appropriate controls should be designed into applications, including user developed applications, to ensure correct processing. These controls should include:

- **Input data validation** – data input to applications should be validated to ensure that it is correct and appropriate.
- **Control of internal processing** – validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
- **Output data validation** – data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

**Process 2.2 – Implement IT Solutions**

This process addresses the implementation of application software and technology infrastructure. New systems need to be made operational once acquired. This requires proper testing, promotion to production, and a post-implementation review.

**Control Objectives**

**Implement IT Solutions (AI2.5, AI3.2, AI3.4, AI7.2 – AI7.9)**

Configure and implement acquired application software and technology infrastructure to meet business objectives. Establish development and test environments and, following testing, control the handover of the system to operations. Perform a post-implementation review and compare behaviour and results to the previous system.
INFORMATION SECURITY CONTROLS

SEPARATION OF DEVELOPMENT AND OPERATIONAL FACILITIES (10.1.4)

Development and operational facilities should be separated to reduce the risks of unauthorised access or changes to the operational system. The following items should be considered:

- Rules for the transfer of software from development to operational status.
- Development and operational software should run on different computers.
- The test environment should emulate the operational system environment as closely as possible.

PROCESS 2.3 – MAINTAIN IT SYSTEMS

This process covers the maintenance and monitoring of application software and technology infrastructure. All changes relating to infrastructure and applications within the production environment are managed in a controlled manner. This process includes defining operating policies and procedures for monitoring infrastructure performance and ensuring preventive maintenance of hardware.

CONTROL OBJECTIVES

MAINTAIN APPLICATION SOFTWARE (AI2.6, AI2.10, AI6.1 – AI6.5)

Develop a strategy and plan for the maintenance of software applications. Set up change management procedures to handle requests for changes to applications and the underlying platforms and update the associated system and user documentation and procedures accordingly whenever changes are implemented.
Maintain technology infrastructure (AI3.3, DS9.1 – DS9.3, DS13.3, DS13.5)

Define and implement procedures to monitor and maintain the technology infrastructure. Maintenance includes patches and upgrades, and maintaining a baseline of configuration items for every system and service as a checkpoint to which to return after changes. Monitor and record all assets and changes to assets and identify personal or unlicensed software.

Information security controls

Change control procedures (10.1.2, 12.5.1)

The implementation of changes should be controlled by the use of formal change control procedures. The procedures should include:

- Ensuring changes are submitted by authorised users.
- Identifying all software, information, database entities and hardware that require amendment.
- Obtaining formal approval before work commences.
- Maintaining an audit trail of all change requests.
- Ensuring that system documentation is updated on the completion of each change.

Inventory of assets (7.1.1)

All assets should be clearly identified and an inventory of all important assets maintained. The asset inventory should include all information necessary to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value.
Equipment maintenance (9.2.4, 12.4.1)

Equipment should be correctly maintained to ensure its continued availability and integrity. The following guidelines should be considered:

- Equipment should be maintained in accordance with the supplier’s recommended service intervals and specifications.
- Only authorised maintenance personnel should carry out repairs and service equipment.
- Records should be kept of all maintenance and suspected or actual faults.

System monitoring and fault logging (10.10.2, 10.10.5)

Procedures for monitoring systems should be established. Areas that should be considered include:

- Authorised access – user IDs, dates and times, types of events, files accessed, etc.
- Unauthorised access attempts – failed or rejected user actions and alerts from proprietary intrusion detection systems.
- System alerts or failures – console alerts or messages, system log exceptions, network management alarms, etc.

Control of technical vulnerabilities (12.6.1)

Timely information about technical vulnerabilities of systems being used should be obtained and appropriate measures taken to address the associated risk. The following guidance should be followed:

- Once a potential technical vulnerability has been identified, the organisation should identify the associated risks and the actions to be
taken. Such action could involve patching of vulnerable systems and/or applying other controls.

- If a patch is available, the risks associated with installing the patch should be assessed.
- Patches should be tested before they are installed. If no patch is available, other controls should be considered, such as:
  1) Turning off services or capabilities related to the vulnerability.
  2) Adapting or adding controls.
  3) Increased monitoring to detect or prevent actual attacks.
  4) Raising awareness of the vulnerability.
- Systems at high risk should be addressed first.

**DOMAIN 3 – DELIVER AND SUPPORT**

This domain is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and operational facilities.

**PROCESS 3.1 – PROVIDE IT SERVICES**

This process addresses the services that IT and third-parties deliver to the business and include the management of third-party services, user training to ensure the proper use of applications and infrastructure, and the timely and effective response to user queries and problems.

**CONTROL OBJECTIVES**

**MANAGE IT SERVICES (DS1.1 – DS1.6)**

Define and agree to service level agreements (SLA) for IT services and regularly review SLAs with internal and external service providers to ensure
that they are effective and up to date and that changes in requirements have been taken into account.

**Manage Third-party Services (DS2.1 – DS2.4)**

Monitor service delivery to ensure that suppliers are meeting current business requirements and continuing to adhere to the contract agreements and SLAs, and that performance is competitive with alternative suppliers and market conditions.

**Perform Training and Create Awareness (AI4.1 – AI4.4, AI7.1, DS7.1 – DS7.3)**

Transfer knowledge and skills to users to allow them to effectively and efficiently use systems and create awareness of information security and other IT related aspects.

**Contend with Incidents and User Queries (DS8.1 – DS8.5, DS10.1 – DS10.4)**

Log and keep track of calls, incidents, service requests and information needs. Incidents that cannot be resolved immediately should be routed to the appropriate party where necessary. Customers should be kept informed of the status of their queries.
INFORMATION SECURITY CONTROLS

IDENTIFICATION OF RISKS RELATED TO EXTERNAL PARTIES (6.2.1)

The risks to the organisation from business processes involving external parties should be identified and appropriate controls implemented before granting access. The identification of risks related to external party access should take into account the following issues:

- The systems an external party is required to access.
- The type of access, e.g. physical access (computers, etc), logical access (databases, etc.), or network connectivity.
- The value and sensitivity of the information involved, and its criticality for business operations.

MONITORING THIRD PARTY SERVICES (10.2.2)

The services, reports and records provided by the third party should be regularly monitored and reviewed. This should involve a service management relationship and process between the organisation and the third party to:

- Monitor service performance levels to check adherence to the agreements.
- Review service reports produced by the third party and arrange regular progress meetings as required by the agreements.
- Provide information about information security incidents and review of this information by the third party and the organisation.
- Review third party audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to the services delivered.
- Resolve and manage any identified problems.
INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING (8.2.2)

All employees of the organisation and, where relevant, contractors and third party users should receive appropriate awareness training. Training should commence with a formal induction process designed to introduce the organisation’s security policies and expectations before access to information or services is granted. Ongoing training should include training in the correct use of systems, e.g. log-on procedures, use of software packages and information on the disciplinary process.

MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENT (13.2.1 – 13.2.2)

Responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents. The following guidelines for information security incident management procedures should be considered:

- Procedures should be established to handle different types of information security incidents, including system failures or loss of service, malicious code and misuse of systems.
- Procedures should cover analysis and identification of the cause of the incident, containment, planning of corrective action to prevent recurrence, communication with those affected by or involved with recovery, and reporting the action to the appropriate authority.
- Audit trails and similar evidence should be collected for internal problem analysis.

The information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents.
**Process 3.2 – Ensure systems security**

Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents. The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures.

**Control objectives**

**Manage security (DS5.1 – DS5.2, DS5.5 – DS5.8, DS5.11)**

Manage IT security by establishing an IT security plan, taking into consideration the IT infrastructure and the security culture. Implement the plan in security policies and communicate security policies and procedures to stakeholders and users.

**Manage user accounts and file access rights (DS5.3 – DS5.4)**

Ensure that all users and their activity on IT systems are uniquely identifiable. Create procedures for creating, suspending, modifying and closing user accounts and related user privileges, and maintain user identities and access rights in a central repository. Ensure that user access rights are requested and approved by management, and perform regular management reviews of all accounts and related privileges.

**Provide virus and spyware protection (DS5.9)**

Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) to protect information systems and technology from malware (e.g. viruses, worms, spyware and spam).
Provide network security (DS5.10)

Use security techniques and related management procedures (e.g. firewalls, security appliances, network segmentation and intrusion detection) to authorise access and control information flow from and to networks.

Ensure physical security (DS12.1 – DS12.5)

Implement physical security measures to secure the physical IT assets. Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, fire and power outages.

Information security controls

User registration (11.2.1)

There should be a formal user registration and de-registration procedure in place for granting and revoking access to all systems. The procedure should include using unique user IDs to enable accountability, removing access rights of users who have changed roles or left the business and removing redundant user IDs and accounts.

Removal of access rights (8.3.3)

The access rights of all users to information and systems should be removed upon termination of their employment, contract or agreement, or adjusted upon change. If a departing user has known passwords for accounts remaining active, these should be changed.
REVIEW OFF USER ACCESS RIGHTS (11.2.2, 11.2.4, 11.5.2)

Management should review users’ access rights at regular intervals using a formal process.

PASSWORD USE (11.2.3, 11.3.1, 11.5.3)

Default vendor passwords should be altered following installation of systems. Users should be required to follow good security practices in the selection and use of password and be advised to keep passwords confidential. A password management system should enforce a choice of quality passwords, enforce regular password changes and prevent reuse of passwords.

UNATTENDED EQUIPMENT (11.3.2)

Users should ensure that unattended equipment has appropriate protection, e.g. logged off or protected with a screensaver.

SECURE LOGON PROCEDURES (11.5.1)

Access to operating systems should be controlled by a secure logon procedure. A good logon procedure should:

- Display a general notice warning that the computer should only be accessed by authorised users.
- Limit the number of unsuccessful logon attempts allowed, e.g. to three attempts, and consider forcing a time delay before further logon attempts are allowed or rejecting further attempts without specific authorisation.
CONTROLS AGAINST MALICIOUS CODE (10.4.1)

Protection against malicious code should be based on malicious code detection and repair software and security awareness. The following guidance should be considered:

- Installation and regular update of malicious code detection and repair software to scan computers and media as a precautionary control, or on a routine basis. The checks carried out should include:
  1) Checking any files on electronic or optical media, and files received over networks, for malicious code before use.
  2) Checking electronic mail attachments and downloads for malicious code before use.
  3) Checking web pages for malicious code.
- Regularly collect information, such as subscribing to mailing lists and/or checking websites giving information about new malicious code.

NETWORK CONTROLS (9.2.3, 10.6.1 – 10.6.2, 11.4.1 – 11.4.2)

Networks should be adequately managed and controlled in order to be protected from threats and to maintain security for the systems using the network. Appropriate logging and monitoring should be applied to enable recording of security relevant actions.

EQUIPMENT SITING AND PROTECTION (9.2.1)

Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access. The following guidelines should be considered:

- Controls should be adopted to minimise the risk of potential physical threats, e.g. theft, fire, water, etc.
• Environmental conditions, such as temperature and humidity, should be monitored.
• Lightning protection filters should be fitted to all incoming communication lines.

**PROCESS 3.3 – ENSURE CONTINUOUS SERVICE**

An effective continuous service process minimises the probability and impact of a major IT service interruption on key business functions and processes. This process addresses developing an IT continuity plan, backup and recovery of data, and utilising offsite backup storage.

**CONTROL OBJECTIVES**

**ENSURE IT CONTINUITY (DS4.1 – DS4.10)**

Develop a disaster recovery and IT contingency plan to reduce the impact of a major disruption on key business functions and processes. The plan should address identification of critical resources, alternative processing and recovery capability of all critical IT services, roles and responsibilities of internal and external service providers, procedures, communication processes, and the testing approach. Test the plan on a regular basis to ensure that IT systems can be effectively recovered. Store offsite all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans.

**MANAGE DATA AND BACKUPS (DS11.1 – DS11.6)**

Define and implement procedures for backup and restoration of systems, applications, data and documentation in line with business requirements and the continuity plan. Maintain an inventory of stored and archived media to ensure their usability and integrity.
INFORMATION SECURITY CONTROLS

SUPPORTING UTILITIES (9.2.2)

Equipment should be protected from power failures. A UPS to support orderly close down or continuous running is recommended for equipment supporting critical business operations.

BUSINESS CONTINUITY MANAGEMENT (9.2.5, 14.1.1 – 14.1.5)

Plans should be developed to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes. The business continuity planning process should consider the following:

• Identification and agreement of all responsibilities and procedures.
• Documentation of agreed procedures and processes.
• Appropriate education of staff in the agreed procedures and processes.
• Testing and updating of the plans.

INFORMATION BACKUP (10.5.1, 10.7.1)

Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure. The following items should be considered:

• The necessary level of backup information should be defined.
• Records of the backup copies and documented restoration procedures should be defined.
• The extent and frequency of backups should reflect the business requirements and the criticality of the information.
• The backups should be stored in a remote location.
Backup media should be given an appropriate level of physical and environmental protection.
Backup media should be regularly tested.

**Domain 4 – Monitor and Evaluate**

All IT processes need to be regularly assessed over time for quality and compliance. This domain addresses performance management, monitoring of internal controls and regulatory compliance.

**Process 4.1 – Monitor IT**

This process provides assurance that information resources supporting business requirements are continually available. It includes reviewing the current performance and capacity of IT resources, relevant performance indicators for IT, the monitoring and reporting of control exceptions, and compliance with laws, regulations and contractual requirements.

**Control Objectives**

**Monitor IT Solutions Performance (DS3.1 – DS3.5)**

Continuously monitor the performance and capacity of IT resources to maintain and tune current performance. Conduct performance and capacity forecasting of IT resources at regular intervals to minimise the risk of service disruptions due to insufficient capacity or performance degradation.

**Monitor IT Performance (ME1.1 – ME1.6, ME2.1 – ME2.7, ME3.1 – ME3.5)**

Measure IT’s solution and service delivery and monitor IT’s contribution to the business by deploying a performance monitoring method (e.g. balanced...
scorecard) that records targets, captures measurements and provides an all-round view of IT performance. Monitor and improve the IT control environment, identify control exceptions, and analyse and identify their underlying root causes. Confirm compliance of IT policies, standards, procedures and methodologies with legal and regulatory requirements.

**INFORMATION SECURITY CONTROLS**

**CAPACITY MANAGEMENT (10.3.1)**

The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

**IDENTIFICATION OF APPLICABLE LEGISLATION (15.1.1 – 15.1.3)**

All relevant statutory, regulatory and contractual requirements should be defined and documented.

**DATA PROTECTION AND PRIVACY OF PERSONAL INFORMATION (15.1.4)**

Data protection and privacy should be ensured as required in relevant legislation and regulations. A data protection and privacy policy should be developed and communicated to all persons involved in the processing of personal information.

This section presented the ITGovSB framework for IT governance in small businesses. In the next section the framework will be assessed in light of the characteristics of IT governance in small businesses.
6.5 Evaluating ITGovSB against the characteristics of IT governance in small businesses

In the previous section the ITGovSB framework for IT governance in small businesses was proposed. The framework was developed to address the seven characteristics of IT governance in small businesses that was discussed in chapter five. This section will evaluate whether the ITGovSB framework effectively addressed or satisfied those characteristics and requirements.

6.5.1 No boards of directors

*An IT governance framework for small businesses will have to make provision for businesses without boards of directors or similar structures.*

ITGovSB makes provision for businesses without boards of directors. Nowhere in the framework is reference made to boards of directors. Where the board of directors is normally responsible for the implementation of IT governance in an organisation, the implementation of ITGovSB is the responsibility of the business owner or CEO, or any senior manager appointed by the owner or CEO.

6.5.2 Limited management structures

*An IT governance framework for small businesses must make provision for businesses with limited management structures.*

Small businesses do not have the extensive management structures of larger organisations. They do not normally have a CIO that can guide the implementation of IT governance. ITGovSB does not refer to CIOs, CFOs, or any such top management positions other than the business owner or CEO. ITGovSB tasks can be performed by the owner or CEO, or any member of staff appointed by the owner of CEO.
6.5.3 Small or non-existent IT departments

An IT governance framework for small businesses should not contain IT jargon and must be simple enough to be understood by non-IT staff or IT staff that do not specialise in IT governance.

Small businesses typically have small or no IT departments, and IT governance might, therefore, have to be implemented by non-IT staff. All the ITGovSB control objectives and controls are clear enough so that it can be understood by non-IT staff. Controls that cannot be physically implemented by non-IT staff are still understandable and easy to communicate to external parties.

6.5.4 Lack of resources

Small businesses need an IT governance framework that is less time-consuming, costs less to implement and can be implemented by fewer employees.

Small businesses typically suffer from a lack of resources. ITGovSB consists of much fewer control objectives and controls than frameworks aimed at large organisations, and can, therefore, be implemented quicker and by fewer employees. This, together with the fact that in most circumstances no external IT governance consultants need to be hired, results in the framework costing less to implement.

6.5.5 Less complex frameworks

Small businesses need an IT governance framework that is simpler and easier to implement, and only contain controls that are applicable to small businesses.
Existing IT governance frameworks are complex and aimed at large organisations. ITGovSB is simpler and easier to implement. It consists of only nine processes, 27 control objectives and 32 controls.

ITGovSB only include control objectives and controls that are applicable to small businesses. As discussed in chapter two, small businesses can vary in size quite considerably. ITGovSB caters for small businesses from one to 50 employees. A business can select and implement only the control objectives and controls that are applicable to that specific business.

6.5.6 Focus on information security

An IT governance framework aimed at small businesses will have to include a strong emphasis on information security and address the common security risks affecting small businesses.

Information security is the biggest IT problem facing small businesses. ITGovSB addresses information security extensively and contains many of the ISO/IEC 27002 information security controls that are applicable to small businesses. The framework addresses the major security risks facing small businesses that were addressed in chapter five.

6.5.7 Low-cost systems

Small businesses should be able to implement an IT governance framework using general end-user software packages such as spreadsheets, word processors and e-mail.

Due to financial and technical constraints, small businesses cannot make use of expensive systems to assist in the implementation of corporate governance. All documentation, policies, etc. that must be
compiled to implement ITGovSB can be done using word processors and spreadsheets, and all communication can be done via e-mail.

The ITGovSB framework effectively addresses the requirements expressed by the seven characteristics of IT governance in small businesses.

6.6 Conclusion

This chapter presented ITGovSB, a framework for IT governance in small businesses.

The ITGovSB framework is based on the CobiT framework and the ISO/IEC 27002 information security controls. It consists of four domains, nine processes, 27 control objectives and 32 information security controls.

By using CobiT and ISO/IEC 27002 together, the benefits of both the wider reference and integrated platform provided by CobiT, and the more detailed guidelines provided by ISO/IEC 27002 is achieved.

Measured against the seven characteristics of IT governance in small businesses, the ITGovSB framework is an effective framework for implementing IT governance in small businesses. In the next chapter, the framework will be evaluated by way of a case study.
Chapter 7

Implementing ITGovSB: A Case Study

7.1 Introduction
7.2 The small business
7.3 The situation before implementing ITGovSB
7.4 The implementation process
7.5 The current situation
7.6 Conclusion
7.1 Introduction

In the previous chapter an IT governance framework for small businesses, ITGovSB, was proposed. The purpose of this chapter is to examine the implementation of the framework at a small business to determine the effectiveness thereof.

In order to follow the case study, it is important to understand the nature and the structure of the business where ITGovSB is implemented and being studied. The chapter will commence by providing background information on ABC Insurance, the small business where the framework is being implemented.

The situation at ABC Insurance before the implementation of ITGovSB will be addressed, followed by the implementation process to date and the current situation of the business. The chapter will conclude by evaluating the implementation of ITGovSB at ABC Insurance.

7.2 The small business

The business where the framework is being implemented, ABC Insurance (fictional name), is an insurance company in Port Elizabeth, South Africa. The company has 13 employees.

The company’s management consists of the CEO, financial manager and marketing manager.

The IT department only has one employee, who reports directly to the CEO. The IT department is responsible for user support, as well as for the development of the in-house administration system and reports.

The company has a service level agreement with a third-party service provider, XYZ Technology (fictional name). One of XYZ Technology’s
engineers is on site for one hour every day to perform maintenance of the network and the servers, and to assist with user support.

ABC Insurance is a small business with few employees, a limited management structure and a small IT department. In the next section the situation at ABC Insurance before the implementation of ITGovSB is addressed.

7.3 The situation before implementing ITGovSB

The IT situation at ABC Insurance before implementing the ITGovSB framework, as well as the reasons why they decided to implement the framework will be addressed in this section.

Before deciding to implement ITGovSB, ABC Insurance did not make use of an IT governance framework. The company’s management was concerned about the way IT was contributing to the business. Most of the IT projects did not complement the business strategy and money was wasted on projects that were started and never completed.

Another concern for management was the way IT was being managed. It was difficult to monitor the performance of the IT department and the IT infrastructure. Although security risks were big, few precautions existed and security issues were addressed mainly retrospectively.

An eye-opener for management was when the company underwent an IT audit as part of the annual financial audit. The IT auditors compiled a report of areas that required attention. The findings and recommendations made by the auditors are listed in Table 7.1.
<table>
<thead>
<tr>
<th>No</th>
<th>Finding</th>
<th>Risk or Effect</th>
<th>Recommendation</th>
</tr>
</thead>
</table>
| 1. | Although the IT department currently makes changes to the in-house developed administration system, these changes are not controlled through a formal change management process. | Risk of unauthorised changes. | A formal change control procedure should be implemented. This should include, inter alia:  
• Formally documenting and approving change requests  
• Separate development and test environments  
• Obtaining user sign-off before transfer to the production environment |
<p>| 2. | Although there is a draft security policy, the policy is not yet completed or implemented. | Without a formal document as guidance, security will be implemented in a haphazard way with the risk of being incomplete. | The IT function, with the involvement and assistance of business management, should define information security policies for the company. Policies should cover accountability, access control, confidentiality, integrity and security management. |
| 3. | There are no formal procedures for the creation of new users or the termination of users who leave the company. | Although the risk is mitigated by the limited staff turnover, there is still a risk of incorrect or unauthorised access. | Formal procedures should be developed to manage the new user administration process. This should include the authorisation of access by business management. A formal process should also be developed for the timely removal of user accounts in respect of employees who have left the company. |
| 4. | There is currently no periodic review of user access rights by the relevant business management. | Incorrect or unauthorised user access could have been granted at the time of creating the users. | User access rights, at all levels, should be formally reviewed and approved by business management on at least a six monthly basis. |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5.</strong></td>
<td><strong>Password and login parameters are not consistently applied to all systems and applications where password authentication is required.</strong></td>
<td><strong>Risk of unauthorised access.</strong></td>
</tr>
<tr>
<td><strong>6.</strong></td>
<td><strong>The servers are housed in a normal office with exterior windows and a normal office door.</strong></td>
<td><strong>If the servers are not adequately protected, they could be at an increased risk of theft or damage.</strong></td>
</tr>
<tr>
<td><strong>7.</strong></td>
<td><strong>The “Administrator” user account on the main authentication server is used by both IT staff members as well as by the support staff from XYZ Technology.</strong></td>
<td><strong>It would not be possible to ensure accountability in the event of a problem or unauthorised actions performed through this powerful user account.</strong></td>
</tr>
<tr>
<td><strong>8.</strong></td>
<td><strong>There are a number of generic user accounts used in Accpac (e.g. User1 &amp; User2).</strong></td>
<td><strong>Generic user accounts prevent accountability, i.e. it would not be possible to establish who processed a particular transaction.</strong></td>
</tr>
</tbody>
</table>

*Table 7.1. Findings and recommendations made by the IT auditors.*
Before deciding to implement ITGovSB, ABC Insurance did not utilise any frameworks to implement IT governance. A number of factors contributed towards their decision to implement ITGovSB, including management concerns and requirements identified by the IT auditors.

7.4 The implementation process

This section will address the implementation of the ITGovSB framework at ABC Insurance. The responsibilities of management and the IT staff will be discussed, as well as the order and priority of the control objectives and the measures taken to implement them.

While the company’s management is responsible for IT governance, the IT department was assigned the task of implementing the controls. The management offered their assistance where needed, and decided to take control in implementing the higher-level controls that affect the overall governance and strategy of the business.

The implementation of ITGovSB at ABC Insurance commenced in March 2008. The implementation of an IT governance framework, even one as uncomplicated as ITGovSB, is a lengthy process. To date, the whole framework has not been implemented yet. This section will report on the controls that have been implemented already, and specify those that are earmarked for future implementation.

ABC Insurance decided to implement the framework in two stages. During stage one, all the control objectives that were necessary to satisfy the requirements of the auditors were implemented. Stage two is still in progress and consists of all the control objectives that are applicable to ABC Insurance that were not implemented during stage one.
7.4.1 Stage one

Stage one consisted of all the control objectives that were identified as a result of the IT audit that was performed at ABC Insurance and took approximately two months to implement. This sub-section will list the control objectives that were implemented during stage one. The implementation of each control objective will be summarised briefly, and the related information security controls that were implemented in achieving the objectives will be referenced.

- **Communicate management support and policies.** This control objective was implemented by developing an information security policy document. The document was approved by management and communicated to all employees. The related information security control is *Information security policy document*.

- **Maintain application software.** Change management procedures were set up to handle requests for changes to applications. Development and operational facilities were also separated. The related information security controls are *Change control procedures* and *Separation of development and operational facilities*.

- **Manage user accounts and file access rights.** Procedures were developed for the creation, modification and termination of user accounts and related user privileges. Password and logon procedures were also created. The related information security controls are *Access control policy*, *User registration*, *Removal of access rights*, *Review of user access rights*, *Password use*, *Unattended equipment* and *Secure logon procedures*. 

• **Ensure physical security.** Physical security measures were implemented to secure the physical IT assets. The servers were placed in a designated server room with no external windows, air-conditioning and fire extinguishers. The related information security control is *Equipment siting and protection*.

The objective of stage one was to satisfy all the requirements that were set by the IT auditors. The next sub-section will address the second stage of the implementation.

### 7.4.2 Stage two

Stage two consists of all the control objectives that are applicable to ABC Insurance that were not implemented during stage one, and has been taking place for the past six months. The control objectives were prioritised according to the management concerns that were identified before the implementation of ITGovSB, as well as the risk to the business should the control objectives not be implemented. Some of the control objectives were already met by existing controls. These control objectives were still documented to formally keep track of the implementation process.

One of the problems that the company’s management identified was that many IT projects were either initiated and never completed, or they did not provide value to the businesses. As a result, the following four control objectives were implemented by management to ensure that IT investments have good business cases and that IT is directed and managed effectively.

• **Provide IT governance.** The IT governance framework was aligned with overall enterprise governance, and management defined the company’s appetite for IT risk.
• **Define an IT strategy.** Management defined an IT strategy that defines how IT goals will contribute to the business’s strategic objectives and created tactical IT plans that are derived from the IT strategic plan.

• **IT planning.** Management and IT analysed available technologies to plan which technological direction is appropriate to realise the defined IT strategy and create business opportunities. They also identified IT risks and assessed the likelihood and impact of all identified risks.

• **Manage the IT budget.** The allocation of IT resources was prioritised and an IT budget reflecting those priorities and the current operating costs were prepared.

The company’s management were also concerned because they did not always have a clear picture as to how the IT department and IT infrastructure are performing. Consequently, the next three control objectives were implemented.

• **Monitor IT solutions performance.** Procedures were put in place to continuously monitor the performance and capacity of IT resources and to conduct performance and capacity forecasting of IT resources at regular intervals to minimise the risk of service disruptions due to insufficient capacity or performance degradation. The related information security control is *Capacity management*.

• **Maintain technology infrastructure.** Procedures were implemented to monitor and maintain the technology infrastructure. The related information security controls are *Inventory of assets, Equipment maintenance, System monitoring and fault logging* and *Control of technical vulnerabilities*.
• **Monitor IT performance.** A balanced scorecard was created that records targets, captures measurements and provides an all-round view of IT performance.

Security is the biggest risk facing small businesses, and the company management were not confident that security controls were adequately implemented. While some of the security-related control objectives were already implemented during stage one, three more were identified and addressed next.

• **Manage security.** An IT security plan was established. Most of the issues were already addressed in the implemented security policies.

• **Provide virus and spyware protection.** Up-to-date anti-virus and anti-spyware software were already present. Automatic weekly and start-up scans were scheduled on all workstations. The related information security control is *Controls against malicious code*.

• **Provide network security.** A firewall was already in place to authorise access and control information flow from and to the network. The related information security control is *Network controls*.

The three other control objectives that were implemented were selected based on the risk that the company would face should the controls not be implemented.

• **Ensure IT continuity.** The company already had an IT contingency plan and stored backup tapes off site. Quarterly tests were scheduled and a UPS was purchased. The related
information security controls are *Supporting utilities* and *Business continuity management*.

- **Manage data and backups.** The company already performed daily backups. Regular backup media tests were scheduled. The related information security control is *Information backup*.

- **Manage the IT department and HR.** Roles and responsibilities were established for the IT department and XYZ Technology’s engineers. Reliance on a single individual performing a critical job function was minimised through knowledge capture and sharing. The related information security controls are *Allocation of information security responsibilities* and *Documenting operating procedures*.

The following control objectives are still to be implemented:

- Identify IT solutions,
- Acquire application software,
- Acquire technological infrastructure,
- Manage IT projects,
- Procure IT solutions,
- Implement IT solutions,
- Manage IT services,
- Manage third-party services,
- Perform training and create awareness, and
- Contend with incidents and user queries.

During stage two, all the control objectives that are applicable to ABC Insurance that were not implemented during stage one has either been implemented or will be implemented in the near future. The control objectives were prioritised based on management concerns and business risk.
While some controls may show immediate results, it will not always be possible to measure the results of all controls immediately. For some controls to be effective, the company must not only implement the controls, but make sure they are strictly enforced. Change management procedures, for example, will prove useless if they are not enforced every time a change is made to systems. Other controls like policies, for instance, have to be kept up-to-date for the control to remain effective.

Thus far, all control objectives have been implemented by the single IT staff member, with the exception of the higher-level control objectives that were driven by management. ITGovSB consists of simple and easy to implement controls. The IT person reported that there were no problems in implementing the controls and that he is capable of implementing the rest of the planned controls without the need for external IT governance consulting.

During the eight months since deciding to implement ITGovSB, the management and IT department at ABC Insurance have implemented a number of the control objectives. During stage one control objectives were implemented to address the findings made by the IT auditors. The focus of stage two is on the control objectives that were identified as a result of management concerns and business risks.

The next section will discuss the current situation at ABC Insurance.

### 7.5 The current situation

Following the implementation of a number of the ITGovSB control objectives, the situation at ABC Insurance is considerably different from what it was eight months ago.

After the implementation of stage one, the requirements and recommendations set by the IT auditors were met. A follow-up meeting with the auditors were scheduled. During this meeting, all the policies and
procedures that were created as part of the implementation were reviewed, and the implemented controls were inspected. The auditors approved the information security policy document and the access control and change management procedures, and they were satisfied that adequate security controls were now in place.

The management of ABC Insurance is satisfied that, as a result of ITGovSB, the IT function is directed and managed well and that the IT strategy and planned IT investments will add value to the business and create a competitive advantage. They also have a clearer picture and a more overall view of the status of the company’s IT function and infrastructure.

With the implementation of ITGovSB, the company has a solid security plan and security controls in place to mitigate the many security risks facing small businesses. While some of the controls were in place already, they are now formally documented. They are easier for the IT department to manage and keep up-to-date, and they provide assurance that the company is protected against these risks. The company is also better equipped to handle any disaster or disruption in business operation.

The implementation process has been very successful and without any issues thus far. ABC Insurance identified five of the characteristics of IT governance in small businesses entrenched in ITGovSB to be of particular value to them.

- **Small or non-existent IT departments.** The IT department at ABC Insurance consists of only one employee. The IT person does not have experience in IT governance, but has thus far understood the processes and control objectives of ITGovSB very well. He feels confident that he can complete the task that has been assigned to him without the assistance of external consultants.

- **Lack of resources.** ITGovSB costs less to implement and can be implemented by fewer employees and in less time than normal IT
governance frameworks. In the eight months that have passed since ABC Insurance decided to implement ITGovSB, roughly two thirds of the control objectives have been implemented already. Most of the controls were implemented by the single IT person during his already busy schedule.

- **Less complex frameworks.** ITGovSB is simple and easy to implement, and only contains controls that are applicable to small businesses. ABC Insurance found that the framework consists of well selected controls and decided to implement all the control objectives. Although the framework is much simpler than other frameworks, the company felt that it still addresses all the key IT governance focus areas.

- **Focus on information security.** ABC Insurance benefited from ITGovSB’s strong focus on information security. After implementing the security-related controls, the requirement set by the IT auditors were met and the overall security risks facing the company were mitigated.

- **Low-cost systems.** All the policies and procedures and other documents that were created so far during implementation were created using word processors and spreadsheets. Staff used e-mail to communicate and schedule meetings.

ABC Insurance has come a long way since deciding to implement ITGovSB and has benefited a great deal from implementing a framework that is aimed at small businesses. The company is in the process of establishing an effective IT governance and internal control structure with the use of ITGovSB and have gained the trust and confidence of both the company’s management and IT auditors. Management is confident that once the entire framework is implemented, complete IT governance will be achieved.
7.6 Conclusion

Before implementing ITGovSB, ABC Insurance did not make use of an IT governance framework. Management realised that the current IT investments were not aligned with the business strategy, and they were concerned about the IT risks that the company was exposed to. Some of these risks were confirmed by the IT auditors.

The implementation of ITGovSB was divided into two stages. Stage one focused on control objectives that were identified as a result of a recent IT audit. Stage two is still in progress and consists of all the control objectives that were not implemented during stage one. In the eight months since ABC Insurance decided to implement ITGovSB, more than two thirds of the control objectives have been implemented.

The implementation of ITGovSB at ABC Insurance has been very successful to date, and both the company’s management and the IT auditors are happy with the results achieved thus far. The implementation is carried out by a small IT department with limited time available, using common word processors and spreadsheet applications. Although ITGovSB is not as complex as existing frameworks, it can be claimed that it is a holistic framework that addresses all the major focus areas of IT governance and has a strong focus on information security.

The objective of this chapter was to assess the effectiveness of ITGovSB by implementing the framework at a small business. While the implementation process is still in progress and many of the implemented control objectives will take time to evaluate, it is clear that ABC Insurance had already benefited greatly from ITGovSB and will continue to realise the benefits in the future.
Chapter 8

Conclusion
8.1 Introduction

The aim of this treatise was to study IT governance in small businesses in order to discover the relevance of IT governance and existing IT governance frameworks to small businesses. IT governance is a subset of corporate governance. It was therefore appropriate to commence by studying corporate governance and its value to small businesses.

Corporate governance is the system by which companies are directed and controlled (Cadbury Committee, 1992, p. 15). While management can be seen as running an organisation, governance is about making sure that the organisation is run properly (Naidoo, 2002, p. 1).

Corporate governance has traditionally been associated with larger organisations only. Recently, however, there has been a need for the application of corporate governance principles in small businesses as well. Small businesses can benefit a great deal from applying corporate governance principles and from the existence of a board of directors (Abor & Biekpe, 2007, p. 296).

IT governance is an essential part of enterprise governance (IT Governance Institute, 2003, p. 10). IT governance consists of the leadership and organisational structures and processes that ensure that the organisation’s IT sustains and extends the organisation’s strategies and objectives (IT Governance Institute, 2003, p. 10).

Just like corporate governance, IT governance is often perceived as something only relevant to larger organisations. This is, however, not the case. IT governance is a key element of every organisation, irrespective of its size (De Graaf, 2008). IT governance is about applying IT in such a way that it creates value for the business, while balancing the risk versus return. Small businesses also want to create value by applying IT (De Graaf, 2008).
IT functions in small businesses differ from those in larger organisations. Small businesses, generally, suffer from a lack of resources and a shortage of skilled IT staff. Due to the differences between IT in small businesses and large organisations, IT governance and the implementation thereof also differs quite considerably between these organisations. Most of the existing IT governance frameworks are intended for large organisations with access to many resources. Small businesses require a simpler framework that is developed specifically for small businesses.

8.2 Summary of chapters

After providing background information on the study area, chapter one stated the research problem and the objectives that had to be achieved to solve the problem. The problem with implementing IT governance in small businesses is that existing IT governance frameworks are intended for large organisations with access to many resources. A less complex IT governance framework that requires fewer resources to implement and is aimed specifically at small businesses was necessary to solve the problem. The primary objective of this treatise was to develop a framework called ITGovSB that small businesses can use to effectively implement IT governance. The secondary objectives were to derive characteristics that define IT governance in small businesses, and to implement the ITGovSB framework at a small business to evaluate its effectiveness.

The objectives of chapter two was to define a small business and to provide some background information about small businesses to reveal the major factors that differentiate small businesses from larger organisations. The various ways of classifying businesses by size and defining small businesses were discussed. For the purpose of this treatise, a small business was defined as any business with 50 employees or less. The important part that small businesses play in the economy, as well as the unique problems that they face were addressed.
Chapter three discussed corporate governance. The purpose of this chapter was to assess whether corporate governance applies, and can offer benefits, to small businesses as well. Corporate governance was defined, and the reasons why companies should maintain good corporate governance principles were discussed. Corporate governance in South Africa, the United States and the United Kingdom was addressed by reviewing, respectively, the King Report on Corporate Governance, the Sarbanes-Oxley Act of 2002 and the Combined Code. It was found that although corporate governance has in the past been associated with large organisations only, it is applicable to small businesses as well. The benefits that corporate governance provides small businesses were discussed.

In chapter four, information on IT governance was provided. IT governance was defined and its objectives and focus areas were discussed. The benefits that successful IT governance can hold for organisations were addressed. The chapter concluded by looking at three of the most widely used frameworks, namely CobiT, the ISO/IEC 27000-series and ITIL.

Chapter five addressed IT governance in the context of small businesses. The purpose of the chapter was to assess whether IT governance is applicable to small businesses as well and, if so, how it differs for small businesses. It was found that IT governance is not only applicable to large organisations, but to small businesses as well. Because of certain factors unique to small businesses, IT governance in the context of small businesses differs quite considerably from that in large organisations. The chapter presented seven characteristics that distinguish IT governance in small businesses from that in large organisations.

The ITGovSB framework was presented in chapter six. The chapter commenced by addressing the reasons why small businesses need an IT governance framework that is specifically adapted for small businesses. The ITGovSB framework is based on the CobiT framework and the ISO/IEC 27002 information security controls. It consists of four domains, nine processes, 27
control objectives and 32 information security controls. The chapter concluded by measuring the effectiveness of ITGovSB against the seven characteristics of IT governance in small businesses that were derived in chapter five.

Chapter seven consisted of a case study. The purpose of the chapter was to examine the implementation of the ITGovSB framework at a small business and to determine the effectiveness thereof. The chapter commenced by providing background information on ABC Insurance, the small business where the framework is being implemented. The situation before the implementation of ITGovSB was addressed, followed by the implementation process to date and the current situation of the business. The chapter concluded by evaluating the implementation of ITGovSB. While the implementation process is still in progress, it was found that ABC Insurance had already benefited greatly from ITGovSB and will continue to realise the benefits in the future.

8.3 Research objectives

Existing IT governance frameworks like CobiT are primarily intended for large organisations with access to many resources, and can be too overwhelming and resource intensive for small businesses to implement (Upfold & Sewry, 2005, p. 5). Small businesses need an IT governance framework that is tailored for small businesses. Such a framework must be less complex and extensive than existing frameworks and require fewer resources to implement.

To provide a solution to the above problem, the ITGovSB framework was developed. The framework is based on CobiT and ISO/IEC 27002, but is less complex and consists of only 27 control objectives and 32 information security controls.
The primary objective of this treatise was to develop a framework that small businesses can use to implement IT governance. This objective was achieved in chapter six with the development of the ITGovSB framework.

In order to achieve the primary objective, it was necessary to understand the differences between IT governance in small businesses and larger organisations. Consequently, one of the secondary objectives of the paper was to derive characteristics that define IT governance in small businesses. In chapter five, seven characteristics of IT governance in small businesses were derived to reach this objective.

Another secondary objective was to implement the ITGovSB framework at a small business to evaluate its effectiveness. In chapter seven, this objective was achieved by implementing the framework at ABC Insurance and reporting on its effectiveness.

8.4 Future research

In chapter seven, the ITGovSB framework was evaluated by means of a case study at ABC Insurance. Although the implementation is still in progress, it was found that the company realised many benefits thus far.

Further research that will be of value includes:

1. Reporting on the implementation and effectiveness of ITGovSB at ABC Insurance once the implementation of the framework is complete, and

2. Performing more case studies at other small businesses to further evaluate the effectiveness of ITGovSB.
8.5 Epilogue

Although IT governance might be perceived as only relevant to large organisations, it is a key element of every organisation, and can assist small businesses in applying IT in such a way that it creates value to the business, while managing the risk.

Small businesses differ from larger organisations in many ways. They make a unique contribution to the economy and they face certain problems that are unique to small businesses. Small businesses also do not possess the many resources of larger organisations. They generally have small or no IT departments and suffer from a lack of finances.

As a result of these differences, IT governance in small businesses differs significantly from large organisations, and existing IT governance frameworks are not suitable for small businesses.

The ITGovSB framework was developed with small businesses in mind. It is less complex than frameworks aimed at large organisations, and requires fewer resources to implement.
References


APPENDIX A

COBIT CONTROL OBJECTIVES AND ISO/IEC 27002 CONTROLS REFERENCED IN ITGovSB

This appendix provides a detailed listing of all the CobiT control objectives and ISO/IEC 27002 information security controls that are referenced in the ITGovSB framework.

The CobiT control objectives that are included in the ISACA survey discussed in chapter five and the information security controls that form part of the ISO/IEC 27002 Information security starting point are also specified.
PROCESS 1.1 – PLAN IT

CONTROL OBJECTIVES

DEFINE AN IT STRATEGY

CobiT control objectives:
PO1.1 IT Value Management
PO1.2 Business-IT Alignment
PO1.3 Assessment of Current Capability and Performance
PO1.4 IT Strategic Plan
PO1.5 IT Tactical Plans
PO1.6 IT Portfolio Management

ISACA survey control objectives:
IT as part of strategic plans – Technologies that support business goals

IT PLANNING

CobiT control objectives:
PO2.1 Enterprise Information Architecture Model
PO2.2 Enterprise Data Dictionary and Data Syntax Rules
PO2.3 Data Classification Scheme
PO2.4 Integrity Management
PO3.1 Technological Direction Planning
PO3.2 Technology Infrastructure Plan
PO3.3 Monitor Future Trends and Regulations
PO3.4 Technology Standards
PO3.5 IT Architecture Board
PO9.1 IT Risk Management Framework
PO9.2 Establishment of Risk Context
PO9.3 Event Identification
PO9.4 Risk Assessment
PO9.5 Risk Response
PO9.6 Maintenance and Monitoring of a Risk Action Plan
ISACA survey control objectives:
Risk evaluation programme – Basic risk assessment and/or self-audits

Provide IT governance

CobiT control objectives:
ME4.1 Establishment of an IT Governance Framework
ME4.2 Strategic Alignment
ME4.3 Value Delivery
ME4.4 Resource Management
ME4.5 Risk Management
ME4.6 Performance Measurement
ME4.7 Independent Assurance

Process 1.2 – Organise and Manage IT

Control objectives

Manage the IT department and HR

CobiT control objectives:
PO4.1 IT Process Framework
PO4.2 IT Strategy Committee
PO4.3 IT Steering Committee
PO4.4 Organisational Placement of the IT Function
PO4.5 IT Organisational Structure
PO4.6 Establishment of Roles and Responsibilities
PO4.7 Responsibility for IT Quality Assurance
PO4.8 Responsibility for Risk, Security and Compliance
PO4.9 Data and System Ownership
PO4.10 Supervision
PO4.11 Segregation of Duties
PO4.12 IT Staffing
PO4.13 Key IT Personnel
PO4.14 Contracted Staff Policies and Procedures
PO4.15 Relationships
PO7.1 Personnel Recruitment and Retention
PO7.2 Personnel Competencies
PO7.3 Staffing of Roles
PO7.4 Personnel Training
PO7.5 Dependence Upon Individuals
PO7.6 Personnel Clearance Procedures
PO7.7 Employee Job Performance Evaluation
PO7.8 Job Change and Termination
PO8.1 Quality Management System
PO8.2 IT Standards and Quality Practices
PO8.3 Development and Acquisition Standards
PO8.4 Customer Focus
PO8.5 Continuous Improvement
PO8.6 Quality Measurement, Monitoring and Review
DS13.1 Operations Procedures and Instructions
DS13.2 Job Scheduling
DS13.4 Sensitive Documents and Output Devices

MANAGE THE IT BUDGET

CobiT control objectives:
PO5.1 Financial Management Framework
PO5.2 Prioritisation Within IT Budget
PO5.3 IT Budgeting
PO5.4 Cost Management
PO5.5 Benefit Management
DS6.1 Definition of Services
DS6.2 IT Accounting
DS6.3 Cost Modelling and Charging
DS6.4 Cost Model Maintenance

MANAGE IT PROJECTS

CobiT control objectives:
PO10.1 Programme Management Framework
PO10.2 Project Management Framework
PO10.3 Project Management Approach
PO10.4 Stakeholder Commitment
PO10.5 Project Scope Statement
PO10.6 Project Phase Initiation
PO10.7 Integrated Project Plan
PO10.8 Project Resources
PO10.9 Project Risk Management
PO10.10 Project Quality Plan
PO10.11 Project Change Control
PO10.12 Project Planning of Assurance Methods
PO10.13 Project Performance Measurement, Reporting and Monitoring
PO10.14 Project Closure

COMMUNICATE MANAGEMENT SUPPORT AND POLICIES

CobiT control objectives:
PO6.1 IT Policy and Control Environment
PO6.2 Enterprise IT Risk and Control Framework
PO6.3 IT Policies Management
PO6.4 Policy, Standard and Procedures Rollout
PO6.5 Communication of IT Objectives and Direction

ISACA survey control objectives:
Management support/buy-in – Leadership from CEO for IT control projects

INFORMATION SECURITY CONTROLS

ALLOCATION OF INFORMATION SECURITY RESPONSIBILITIES

ISO/IEC 27002 controls:
6.1.3 Allocation of information security responsibilities
8.1.1 Roles and responsibilities

ISO/IEC 27002 Information security starting point controls:
6.1.3 Allocation of information security responsibilities
SCREENINGS

ISO/IEC 27002 controls:
8.1.2 Screening

DOCUMENTING OPERATING PROCEDURES

ISO/IEC 27002 controls:
10.1.1 Documented operating procedures

INFORMATION SECURITY POLICY DOCUMENT

ISO/IEC 27002 controls:
5.1.1 Information security policy document
5.1.2 Review of the information security policy
6.1.1 Management commitment to information security

ISO/IEC 27002 Information security starting point controls:
5.1.1 Information security policy document

ACCESS CONTROL POLICY

ISO/IEC 27002 controls:
11.1.1 Access control policy

PROCESS 2.1 – ACQUIRE IT SOLUTIONS

CONTROL OBJECTIVES

IDENTIFY IT SOLUTIONS

CobiT control objectives:
AI1.1 Definition and Maintenance of Business Functional and Technical Requirements
AI1.2 Risk Analysis Report
AI1.3 Feasibility Study and Formulation of Alternative Courses of Action
AI1.4 Requirements and Feasibility Decision and Approval

ACQUIRE APPLICATION SOFTWARE

CobiT control objectives:
AI2.1 High-level Design
AI2.2 Detailed Design
AI2.3 Application Control and Auditability
AI2.4 Application Security and Availability
AI2.7 Development of Application Software
AI2.8 Software Quality Assurance
AI2.9 Applications Requirements Management

ISACA survey control objectives:
Data input controls – Field formats, periodic data range testing

ACQUIRE TECHNOLOGICAL INFRASTRUCTURE

CobiT control objectives:
AI3.1 Technological Infrastructure Acquisition Plan

PROCURE IT SOLUTIONS

CobiT control objectives:
AI5.1 Procurement Control
AI5.2 Supplier Contract Management
AI5.3 Supplier Selection
AI5.4 IT Resources Acquisition

INFORMATION SECURITY CONTROLS

SECURITY REQUIREMENTS ANALYSIS

ISO/IEC 27002 controls:
12.1.1 Security requirements analysis and specification
CORRECT PROCESSING IN APPLICATIONS

ISO/IEC 27002 controls:
12.2.1 Input data validation
12.2.2 Control of internal processing
12.2.3 Message integrity
12.2.4 Output data validation
12.5.5 Outsourced software development

ISO/IEC 27002 Information security starting point controls:
12.2 Correct processing in applications

PROCESS 2.2 – IMPLEMENT IT SOLUTIONS

CONTROL OBJECTIVES

IMPLEMENT IT SOLUTIONS

CobiT control objectives:
AI2.5 Configuration and Implementation of Acquired Application Software
AI3.2 Infrastructure Resource Protection and Availability
AI3.4 Feasibility Test Environment
AI7.2 Test Plan
AI7.3 Implementation Plan
AI7.4 Test Environment
AI7.5 System and Data Conversion
AI7.6 Testing of Changes
AI7.7 Final Acceptance Test
AI7.8 Promotion to Production
AI7.9 Post-implementation Review
INFORMATION SECURITY CONTROLS

SEPARATION OF DEVELOPMENT AND OPERATIONAL FACILITIES

ISO/IEC 27002 controls:
10.1.4 Separation of development, test, and operational facilities

PROCESS 2.3 – MAINTAIN IT SYSTEMS

CONTROL OBJECTIVES

MAINTAIN APPLICATION SOFTWARE

CobiT control objectives:
AI2.6 Major Upgrades to Existing Systems
AI2.10 Application Software Maintenance
AI6.1 Change Standards and Procedures
AI6.2 Impact Assessment, Prioritisation and Authorisation
AI6.3 Emergency Changes
AI6.4 Change Status Tracking and Reporting
AI6.5 Change Closure and Documentation

MAINTAIN TECHNOLOGY INFRASTRUCTURE

CobiT control objectives:
AI3.3 Infrastructure Maintenance
DS9.1 Configuration Repository and Baseline
DS9.2 Identification and Maintenance of Configuration Items
DS9.3 Configuration Integrity Review
DS13.3 IT Infrastructure Monitoring
DS13.5 Preventive Maintenance for Hardware
INFORMATION SECURITY CONTROLS

CHANGE CONTROL PROCEDURES

ISO/IEC 27002 controls:
10.1.2 Change management
12.5.1 Change control procedures

INVENTORY OF ASSETS

ISO/IEC 27002 controls:
7.1.1 Inventory of assets

EQUIPMENT MAINTENANCE

ISO/IEC 27002 controls:
9.2.4 Equipment maintenance
12.4.1 Control of operational software

SYSTEM MONITORING AND FAULT LOGGING

ISO/IEC 27002 controls:
10.10.2 Monitoring system use
10.10.5 Fault logging

CONTROL OF TECHNICAL VULNERABILITIES

ISO/IEC 27002 controls:
12.6.1 Control of technical vulnerabilities

ISO/IEC 27002 Information security starting point controls:
12.6 Control of technical vulnerabilities
PROCESS 3.1 – PROVIDE IT SERVICES

CONTROL OBJECTIVES

MANAGE IT SERVICES

CobiT control objectives:
DS1.1 Service Level Management Framework
DS1.2 Definition of Services
DS1.3 Service Level Agreements
DS1.4 Operating Level Agreements
DS1.5 Monitoring and Reporting of Service Level Achievements
DS1.6 Review of Service Level Agreements and Contracts

MANAGE THIRD-PARTY SERVICES

CobiT control objectives:
DS2.1 Identification of All Supplier Relationships
DS2.2 Supplier Relationship Management
DS2.3 Supplier Risk Management
DS2.4 Supplier Performance Monitoring

PERFORM TRAINING AND CREATE AWARENESS

CobiT control objectives:
AI4.1 Planning for Operational Solutions
AI4.2 Knowledge Transfer to Business Management
AI4.3 Knowledge Transfer to End Users
AI4.4 Knowledge Transfer to Operations and Support Staff
AI7.1 Training
DS7.1 Identification of Education and Training Needs
DS7.2 Delivery of Training and Education
DS7.3 Evaluation of Training Received

ISACA survey control objectives:
Employee IT security training – Training for e-mail, Web, and password use
CONTEND WITH INCIDENTS AND USER QUERIES

CobiT control objectives:
DS8.1 Service Desk
DS8.2 Registration of Customer Queries
DS8.3 Incident Escalation
DS8.4 Incident Closure
DS8.5 Reporting and Trend Analysis
DS10.1 Identification and Classification of Problems
DS10.2 Problem Tracking and Resolution
DS10.3 Problem Closure
DS10.4 Integration of Configuration, Incident and Problem Management

INFORMATION SECURITY CONTROLS

IDENTIFICATION OF RISKS RELATED TO EXTERNAL PARTIES

ISO/IEC 27002 controls:
6.2.1 Identification of risks related to external parties

MONITORING THIRD PARTY SERVICES

ISO/IEC 27002 controls:
10.2.2 Monitoring and review of third party services

INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING

ISO/IEC 27002 controls:
8.2.2 Information security awareness, education and training

ISO/IEC 27002 Information security starting point controls:
8.2.2 Information security awareness, education and training
Management of Information Security Incidents and Improvement

ISO/IEC 27002 controls:
13.2.1 Responsibilities and procedures
13.2.2 Learning from information security incidents

ISO/IEC 27002 Information security starting point controls:
13.2 Management of information security incidents and improvements

Process 3.2 – Ensure Systems Security

Control Objectives

Manage Security

CobiT control objectives:
DS5.1 Management of IT Security
DS5.2 IT Security Plan
DS5.5 Security Testing, Surveillance and Monitoring
DS5.6 Security Incident Definition
DS5.7 Protection of Security Technology
DS5.8 Cryptographic Key Management
DS5.11 Exchange of Sensitive Data

Manage User Accounts and File Access Rights

CobiT control objectives:
DS5.3 Identity Management
DS5.4 User Account Management

ISACA survey control objectives:
File access privilege controls – Role-based access control, least privilege
ID and authorization procedures – Complex passwords, password change policies
PROVIDE VIRUS AND ANTI-SPYWARE PROTECTION

CobiT control objectives:
DS5.9 Malicious Software Prevention, Detection and Correction

ISACA survey control objectives:
Virus protection – Updated anti-virus, anti-spyware applications

PROVIDE NETWORK SECURITY

CobiT control objectives:
DS5.10 Network Security

ISACA survey control objectives:
Network security – Updated firewall, secure wireless transmissions

ENSURE PHYSICAL SECURITY

CobiT control objectives:
DS12.1 Site Selection and Layout
DS12.2 Physical Security Measures
DS12.3 Physical Access
DS12.4 Protection Against Environmental Factors
DS12.5 Physical Facilities Management

INFORMATION SECURITY CONTROLS

USER REGISTRATION

ISO/IEC 27002 controls:
11.2.1 User registration
REMOVAL OF ACCESS RIGHTS

ISO/IEC 27002 controls:
8.3.3 Removal of access rights

REVIEW OF USER ACCESS RIGHTS

ISO/IEC 27002 controls:
11.2.2 Privilege management
11.2.4 Review of user access rights
11.5.2 User identification and authentication

PASSWORD USE

ISO/IEC 27002 controls:
11.2.3 User password management
11.3.1 Password use
11.5.3 Password management system

UNATTENDED EQUIPMENT

ISO/IEC 27002 controls:
11.3.2 Unattended user equipment

SECURE LOGON PROCEDURES

ISO/IEC 27002 controls:
11.5.1 Secure log-on procedures

CONTROLS AGAINST MALICIOUS CODE

ISO/IEC 27002 controls:
10.4.1 Controls against malicious code
NETWORK CONTROLS

ISO/IEC 27002 controls:
9.2.3 Cabling security
10.6.1 Network controls
10.6.2 Security of network services
11.4.1 Policy on use of network services
11.4.2 User authentication for external connections

EQUIPMENT SITING AND PROTECTION

ISO/IEC 27002 controls:
9.2.1 Equipment siting and protection

PROCESS 3.3 – ENSURE CONTINUOUS SERVICE

CONTROL OBJECTIVES

ENSURE IT CONTINUITY

CobiT control objectives:
DS4.1 IT Continuity Framework
DS4.2 IT Continuity Plans
DS4.3 Critical IT Resources
DS4.4 Maintenance of the IT Continuity Plan
DS4.5 Testing of the IT Continuity Plan
DS4.6 IT Continuity Plan Training
DS4.7 Distribution of the IT Continuity Plan
DS4.8 IT Services Recovery and Resumption
DS4.9 Offsite Backup Storage
DS4.10 Post-resumption Review

ISACA survey control objectives:
IT continuity and recovery plan – Basic disaster recovery plan (DRP) procedures
MANAGE DATA AND BACKUPS

CobiT control objectives:
DS11.1 Business Requirements for Data Management
DS11.2 Storage and Retention Arrangements
DS11.3 Media Library Management System
DS11.4 Disposal
DS11.5 Backup and Restoration
DS11.6 Security Requirements for Data Management

ISACA survey control objectives:
Backups – Regular and tested backup procedures

INFORMATION SECURITY CONTROLS

SUPPORTING UTILITIES

ISO/IEC 27002 controls:
9.2.2 Supporting utilities

BUSINESS CONTINUITY MANAGEMENT

ISO/IEC 27002 controls:
9.2.5 Security of equipment off-premises
14.1.1 Including information security in the business continuity management process
14.1.2 Business continuity and risk management
14.1.3 Developing and implementing continuity plans including information security
14.1.4 Business continuity planning framework
14.1.5 Testing, maintaining and re-assessing business continuity plans

ISO/IEC 27002 Information security starting point controls:
14 Business continuity management
INFORMATION BACKUP

ISO/IEC 27002 controls:
10.5.1 Information back-up
10.7.1 Management of removable media

PROCESS 4.1 – MONITOR IT

CONTROL OBJECTIVES

MONITOR IT SOLUTIONS PERFORMANCE

CobiT control objectives:
DS3.1 Performance and Capacity Planning
DS3.2 Current Performance and Capacity
DS3.3 Future Performance and Capacity
DS3.4 IT Resources Availability
DS3.5 Monitoring and Reporting

MONITOR IT PERFORMANCE

CobiT control objectives:
ME1.1 Monitoring Approach
ME1.2 Definition and Collection of Monitoring Data
ME1.3 Monitoring Method
ME1.4 Performance Assessment
ME1.5 Board and Executive Reporting
ME1.6 Remedial Actions
ME2.1 Monitoring of Internal Control Framework
ME2.2 Supervisory Review
ME2.3 Control Exceptions
ME2.4 Control Self-assessment
ME2.5 Assurance of Internal Control
ME2.6 Internal Control at Third Parties
ME2.7 Remedial Actions
ME3.1 Identification of External Legal, Regulatory and Contractual Compliance Requirements
ME3.2 Optimisation of Response to External Requirements
ME3.3 Evaluation of Compliance With External Requirements
ME3.4 Positive Assurance of Compliance
ME3.5 Integrated Reporting

**INFORMATION SECURITY CONTROLS**

**CAPACITY MANAGEMENT**

ISO/IEC 27002 controls:
10.3.1 Capacity management

**IDENTIFICATION OF APPLICABLE LEGISLATION**

ISO/IEC 27002 controls:
15.1.1 Identification of applicable legislation
15.1.2 Intellectual property rights (IPR)
15.1.3 Protection of organisational records

**DATA PROTECTION AND PRIVACY OF PERSONAL INFORMATION**

ISO/IEC 27002 controls:
15.1.4 Data protection and privacy of personal information

ISO/IEC 27002 Information security starting point controls:
15.1.4 Data protection and privacy of personal information