SCHOOL OF INFORMATION TECHNOLOGY

PERSONAL DETAILS	
STUDENT NUMBER	s20066407
SURNAME	Wessels
FIRST NAME	Eugene
TELEPHONE	0846035804
POSTAL ADDRESS	P.O. Box 460, Raslouw, 0109, South Africa
RESEARCH DETAILS	
DEGREE	MASTERS OF COMMERCI (INFORMATICS)
DEPARTMENT	INFORMATICS, UNIVERSITY OF PRETORIA
SUPERVISOR	Dr. J.J. van Loggerenberg
CO-SUPERVISOR	
TITLE	Towards a framework for business continuity management: an IT governance perspective

DECLARATION BY CANDIDATE
I declare that this research, submitted by me, is my own work, that I have referenced all the sources that I have used and that no part was previously submitted at any tertiary institution.

DECLARATION BY SUPERVISOR (AND CO-SUPERVISOR)
I declare herewith that I approve the submission of this research.

REQUIRED SIGNATURES			
STUDENT		**DATE**	
SUPERVISOR		**DATE**	
CO-SUPERVISOR		**DATE**	

TOWARDS A FRAMEWORK FOR BUSINESS CONTINUITY MANAGEMENT: AN IT GOVERNANCE PERSPECTIVE

Full Thesis By

EUGENE WESSELS (s20066407)

Submitted in fulfilment of the requirements for the degree of

MASTERS OF COMMERCI (INFORMATICS)

in the

DEPARTMENT OF INFORMATICS

SCHOOL OF INFORMATION TECHNOLOGY

of the

FACULTY OF BUSINESS AND MANAGEMENT, UNIVERSITY OF PRETORIA

Supervisor:

Dr. J.J van Loggerenberg

Date of Submission:

2006-12-01

NOMINATION OF EXTERNAL EXAMINER

UNIVERSITY	University of Pretoria	**DEPARTMENT**	Informatics
MODULE:	INF890 Full thesis with summarised article.		

CANDIDATE	**STUDENT NUMBER**	**SUPERVISOR**	**CO-SUPERVISOR**
E.Wessels	S20066407	Dr. J.J van Loggerenberg	

EXTERNAL EXAMINER	
NAME	
QUALIFICATION	
POSTAL ADDRESS	
CONTACT NUMBER	
E-MAIL ADDRESS	

SIGNATURES OF DEPARTMENT OF INFORMATICS REPRESENTATIVES			
POST GRADUATE MANAGER		**DATE**	
HOD		**DATE**	

CONTENTS

ABSTRACT

The concept of business continuity management has gained wide acceptance in recent years. Recent natural disasters such as the 2004 tsunami and terrorist activities such as the 911 World Trade Centre bombing, has emphasised the importance of business continuity management. Many of these events had catastrophic consequences, which left most executives faced with the challenge of improving the continuity of their organisation. Not to long ago, these executives were also faced with the challenge of managing their IT investments in such a way that it is aligned with the strategic goals of the organisation. An initiative referred to as IT governance was developed and IT governance frameworks instantly assisted executives to obtain direct business value from IT investments. The problem statement addressed in this research is the lack of a generally accepted business continuity management framework. This research aims to leverage of the success of IT governance in an attempt to establish the beginnings of a framework for business continuity management. In addition, the research also illustrates a paradigm shift where the enterprise continuity of a typical organisation has evolved from disaster recovery to business continuity management. The research approach executed is based on the interpretivism paradigm and is used to interpret the results of the research methodology and research method. The research methodology consists of a literature survey and empirical study whereas a content analysis is used as the research method.

Key Words: Business Continuity Management, Disaster Recovery, IT Governance, COBIT, ITIL, Content Analysis

CHAPTER 1
BACKGROUND AND RESEARCH OBJECTIVES

1.1 INTRODUCTION

Many executives face the daunting challenge of ensuring the continuity of their organisation while governing IT effectively and efficiently. Recent disasters and attacks have had devastating effects on well-established organisations globally. Most of these organisations suffered significant losses, which dramatically influenced the future of their existence – others were simply unable to recover. Tragically, a number of selected organisations suffered numerous fatalities. Not many years ago, organisations experienced IT related challenges similar to the business continuity management dilemmas faced today. Organisations invested heavily in IT infrastructures but received minimal return on investments. The benefits promised by some IT implementations never materialised. At times, IT projects were not even completed, resulting in substantial financial losses. Recently, IT governance frameworks have emerged to ease some of the IT related challenges experienced by organisations. These frameworks have been successfully accepted and implemented by practitioners and evidence show that many of the original challenges experienced have now been resolved.

Unlike IT governance, no formal business continuity management frameworks have emerged that are generally available and accepted by organisations. This research aims to leverage of the success of IT governance in an attempt to establish the beginnings of a framework for business continuity management.

Chapter one presents information on the details of the research. Specifically, this chapter discusses the problem statement, research objectives, research approach and overview of the succeeding chapters.

1.2 BACKGROUND

Business continuity management and information technology (IT) governance are concepts that have both undergone vast transformations in recent years. The introduction of IT in organisations has fundamentally transformed the manner in which business activities are supported and conducted. Consequently, the continued existence of most modern organisations has become dependant on their IT infrastructure. This has resulted in the emphasis being placed on the effective and efficient governance of IT investments with the aim of ensuring, amongst others, the continuity of organisations.

1.2.1 INTRODUCING BUSINESS CONTINUITY MANAGEMENT AND IT GOVERNANCE

Business continuity management is defined as the measures and technology an organisation puts in place to withstand malicious attacks (Price 2004:34). Examples of malicious attacks include hacking, viruses and infrastructure disasters whereas technological measures to prevent these examples range from security to archiving and recovery. Governments have recognised the importance of business continuity management in organisations, resulting in acts like Sarbanes-Oxley (Graham & Kaye, 2006:295) and guidelines like the King II Report in South Africa. The acts force organisations to create IT controls and compliances that form the basis of any organisation's IT governance framework (Damianides, 2005:77).

Gaynor (2002:28) defines IT governance as a process of aligning IT initiatives with organisational strategy while minimising IT related risks through best practices. To make it easier to understand and implement, IT governance frameworks such as the Control Objectives for Information and Related Technology (Cobit) and IT Infrastructure Library (ITIL) have been developed over the years (Carroll *et al.*, 2004:233). These frameworks are considered best practice for IT operations, procedures and standards with the aim of ensuring, amongst others, an organisation's business continuity, albeit from an IT perspective. However, as stated by Koch (2002), IT governance is often more philosophical than practical. The increasing number of publications

about the inconsistencies and failures of IT governance (Hoffman, 2003:14; Hoffman, 2004:6) supports this. These publications raise the suspicion of the failure of certain IT governance elements of which the assurance of IT continuity might be one example.

Even though both business continuity management and IT governance have been discussed and explored in the literature, a limited number of academic publications exist that explore both business continuity management and IT governance in detail. In this research, the relationship between business continuity management and IT governance is explored together with the aspects within IT governance frameworks that contribute towards business continuity management. These results are used to develop a framework for business continuity management.

1.2.2 EXAMPLES ILLUSTRATING THE IMPORTANCE OF BUSINESS CONTNUITY MANAGEMENT AND IT GOVERNANCE

In recent years, many events have influenced the continuity of organisations, ranging from natural disasters to terrorist attacks and even deliberate malicious events executed by man. Graham & Kaye (2006:5) go as far as stating that the world has become 'riskier'. Hiles & Barnes (2001:68) emphasise the importance of business continuity management by explaining that 43% of companies that have suffered a disaster, never fully recover. By presenting a few examples below, this research aims to illustrate the importance of business continuity management and IT governance.

- At the turn of the century, a global fear threatened the entire business world as organisations questioned whether their Information Systems (IS) were compatible with the new millennium (Calderon & Dishovska, 2005:21). The problem became known as the Y2K bug and, collectively, organisations spent billions to correct the problem. Manning (1999:243) describes this event as the first 'global exercise in business continuity [management]';

- Enron, one of the biggest organisations in the history of the world, declared bankruptcy despite of its assets worth 63.4 billion dollars. The share price of Enron dropped from 90 dollar a share to less than one dollar a share. The cause of the Enron debacle was financially related, specifically on the accounting principles followed (Benston & Hartgraves, 2002:105);

- On the night of the 17th of March 2000, a thunderstorm stuck a manufacturing plant of Philips. Even though the damage caused by the fire seemed limited and harmless, the smoke of the fire destroyed millions of mobile computer chips. The result of the incident was not limited to Philips' loss of 40 million dollars in sales. At the time of the disaster, this particular manufacturing plant was the sole provider of the electronic chips used by the Ericsson. As a result of the unavailability of the chips, Ericsson's mobile division announced a loss of 2.34 billion dollars within nine months. In April the following year, Ericsson's plans to withdraw from the mobile industry were halted when they signed a joint venture with Sony, resulting in the 50-50 ownership called Sony-Ericsson (Sheffi, 2005: 9);

- On 2nd of September 2001, Baxter International who had earlier acquired Althin Medical AB, announced that the dialysis filter manufactured by Althin had a defect. A well-established plant used a particular liquid during the quality-control processes. Even though the liquid had been successfully used before, specific factors contributed to the liquid causing defects with the dialysis, resulting in the death of more than 50 patients. The consequence of the disaster caused Baxter to announce a 189 million dollar loss to its bottom line as a result of the recovery from the defective filters. The loss was almost double the value of the acquisition of Althin (Sheffi, 2005: 154);

- On the 11th of September 2001, a terrorist attack destroyed the World Trade Centres of the United States of America. Cantor Fitzgerald, a bond trading company, lost 658 employees. It was not only the tragedy

of the losing the employees that influenced the company. The loss of the internal knowledge and client relationships also had a severe impact on the company. In addition, Cantor Fitzgerald could only recover two months after the attack to its trillion dollars a week trading activities, losing millions of dollars as a direct result of the attack (Sheffi, 2005: 236). Besides Cantor Fitzgerald, the city of New York estimated losses in the area of 100 billion dollars as a result of the terrorist attack (Rutherford *et al.*, 2002:4);

- In January 2003, the SQL Slammer computer worm was released through the internet which, in a matter of days, infected millions of computers. Examples of the devastating effect of Slammer were the disablement of Seattle's emergency call centre and the discontinuation of 13,000 automated teller machines of the Bank of America. In total, the damage of the worm was estimated to be in the region of one billion dollars (Sheffi, 2005: 30);

- On the 8th of May 2003, a devastating tornado hit Oklahoma City and destroyed an assembly plant of General Motors, resulting in a loss between 140 to 200 million dollars and having serious implications to the clients of and suppliers to General Motors (Sheffi, 2005: 29); and

- Lastly, when hurricane Katrina hit the Gulf Cost of the United States of America in August 2005, it was described as America's most destructive natural disaster ever. The hurricane completely destroyed several communities, killing 1,300 people, displacing two million people and demolishing 350,000 homes. The total cost of hurricane Katrina is estimated to be in the region of 100 billion dollars (Rodriguez & Marks, 2006: 5).

From these examples, the criticality of both business continuity management and IT governance are illustrated. The impact of some of the technical examples, like the Y2K bug and the SQL Slammer computer worm, could have been minimised by the effective and efficient governance of IT whereas

effective business continuity management could have prevented the discontinuation of many of these organisations. The consequences of these examples clearly indicate how an unanticipated disruption can destroy a well-established organisation in a very short time period.

1.3 PROBLEM STATEMENT

The concept of business continuity management has gained momentum in recent years. Natural disasters, terrorist activities and malicious events have emphasised the importance of business continuity management. This has resulted in practitioners and less so academics, to vigorously publish articles in an attempt to transform what Price (2004:34) calls an 'obscure initiative' to a 'role of prominence' in the practice of IT and business. The authors often originated from different disciplines and, as a result, approached the topic from different angles. For instance, when authors from the field of Information Systems address the topic, they tend to take a technical view of business continuity management namely disaster recovery. Likewise, when authors from the risk management field address the issue, they tend to focus more strongly on risk management, sometimes to the exclusion of other aspects. Consequently, many different perceptions of business continuity management currently exist (Hiles & Barnes, 2001:43), resulting in the definition to be vague and its objectives to be inconsistent. The result is that the concept of business continuity management is interpreted and described in a variety of ways. Business continuity management is often equated with disaster recovery, business recovery, business recovery planning, business resumption planning, risk management, crisis management and contingency planning – where each term differs in principle and scope. What seems to be seriously lacking is an accepted, underlying and unifying theory of business continuity management.

Similar to business continuity management, the importance of IT governance in organisations has also increased in recent years. The main aim of IT governance is to align IT initiatives with business strategy (Van Grembergen, 2003: 242). IT governance propagates the delivery of numerous benefits to

organisations when implemented correctly. One such example is the continuous sustainability of an organisation's IT infrastructure, an aspect which fundamentally forms the essence of an organisation's continuity, at least from an IT perspective. This is proven by the existence of IT governance processes dedicated to the continuity of Information Systems, as recognised by the two popular IT governance frameworks, namely COBIT and ITIL. Organisations worldwide have implemented COBIT and ITIL with much success. Unfortunately, the majority of IT governance publications are still practitioner-oriented and only a limited number of publications are academically accredited (Carroll *et al.*, 2004:239). Although neither of the IT governance frameworks are academically accredited material, each framework can contribute significantly towards this research.

Even though various literature sources on business continuity management were identified, very few are of a rigorous academic nature. Compared to other Information Systems research topics, very few books on IT governance and business continuity management have been published. The majority of literature available is in the form of articles. From this limited amount of publications, inconsistent terminologies and objectives are used by the authors when referring to the concept of business continuity management. Furthermore, the researcher is unaware of any business continuity management frameworks similar to those proposed for IT governance.

The problem statement addressed in this research is the absence of a theoretically sound business continuity management framework. Consequently, the researcher suspects the frameworks developed by practitioners to be mostly incomplete, incompatible and perhaps even conflicting. Examples of practitioners' frameworks are discussed in the empirical study presented in chapter seven. No academics have, to date and to the knowledge of the researcher, developed a generally accepted theoretical framework to practise business continuity management. The definition of business continuity management proposed by Graham & Kaye (2006:10) makes reference to 'a framework', but a generally accepted and accredited business continuity management framework does not exist. The

researcher is concerned about the completeness of the existing business continuity management frameworks used by organisations, bearing in mind that confusion exists on the topic. At the very least, this research aims to emphasise the lack of a formal and generally accepted business continuity management framework (similar to the COBIT and ITIL IT governance frameworks). By determining the definition and objectives of business continuity management, this research aims to develop a more academically based business continuity management framework. In doing so, the research aims to address the confusion around business continuity management in hope of ultimately increasing the sustainability of organisations.

1.4 RESEARCH OBJECTIVES

The problem statement highlights the lack of a theoretical business continuity management framework. The research objective is to initiate the development of a sound business continuity management framework. The research does so by utilising as a base what is specified and implied of business continuity management in globally accepted IT governance frameworks. Through the investigation of the relationship between business continuity management and IT governance, the research identifies what IT governance frameworks contribute towards business continuity management. By analysing those specific components of the IT governance frameworks dealing with business continuity, the objective and detailed objectives of business continuity management are derived through the viewpoint of IT governance. The objective of business continuity management defines and identifies the purpose of business continuity management. The detailed objectives of business continuity management are sub activities that contribute towards the achievement of the main objective. The objective and detailed objectives are used to development a business continuity management framework.

1.4.1 MAIN RESEARCH QUESTION

How does a framework for business continuity management look like when it is based upon a sound theoretical basis?

1.4.2 SECONDARY RESEARCH QUESTION

In an attempt to answer the main research question, the following secondary research questions are answered:

- What is the definition of IT governance?
- What are the advantages IT governance claims to offer?
- What IT governance frameworks exist and how do they compare with each other?
- How has IT governance and business continuity management evolved in recent years?
- What is the relationship between IT governance and business continuity management?
- Which processes within IT governance frameworks contribute towards business continuity management?
- What is the objective of business continuity management?
- What are the detailed objectives of business continuity management?
- Who are the typical role players responsible for business continuity management?
- How should business continuity management be integrated with the different IT governance frameworks?

1.5 RESEARCH APPROACH

This section discusses the research approach, which is presented in Figure 1: A paradigm serves as the foundation for the research approach and is extended by a methodology. Based on the methodology, a specific research method is followed. Figure 2 displays the execution of the research approach in more detail.

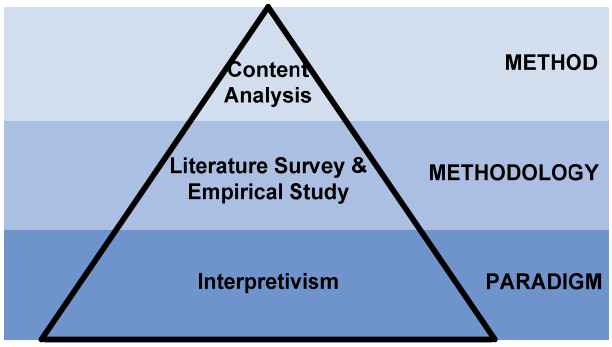

Figure 1: Research Approach

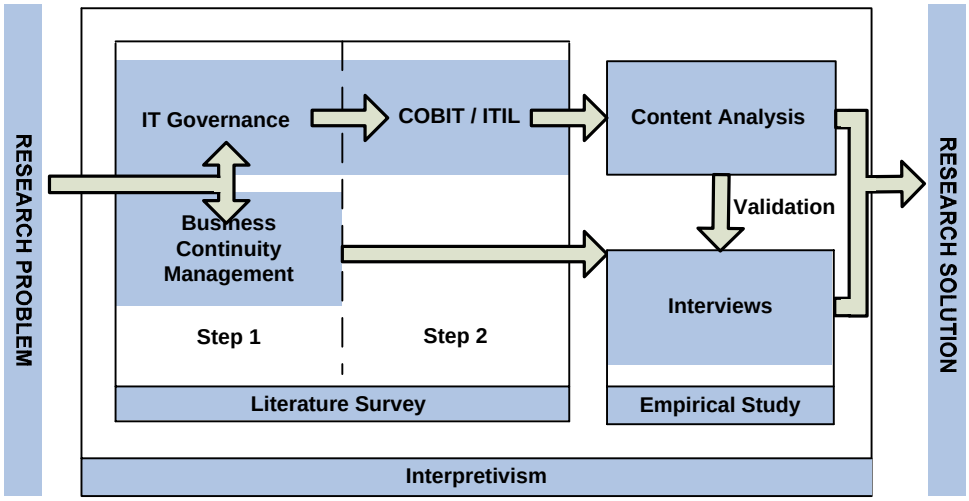

Figure 2: Research Approach Execution Details

1.5.1 PARADIGM

As pointed out by Bandarouk & Ruel (2004), interpretive research has gained significant acceptance since the 1990's as an alternative to the traditional positivist approach. The researcher is of the opinion that both the lack of interpretation and static nature of positivism disqualify it as an approach to study this Information System research topic. Instead, the characteristics of interpretivism such as being relative, conceptual and dynamic act as

motivation for selecting interpretivism as the paradigm to investigate the research problem. The interpretivism paradigm used in this research follows a qualitative approach in order to gain an understanding, rather than an explanation, of the research problem.

The remaining parts of the research approach are based on the interpretivism paradigm. The results of the literature survey, empirical study and content analysis are processed in an interpretative manner. Unlike the methodology and method used in this research, the paradigm of interpretivism is not an activity but rather a specific manner in which the information derived is conceptualised.

1.5.2 METHODOLOGY

The research methodology consists of both a literature survey and empirical study. The research commences with the completion of a literature survey that serves as basis for the rest of the research.

1.5.2.1 LITERATURE SURVEY

Publications on IT governance and business continuity management are investigated in an attempt to answer the main research question. The literature survey is divided into two steps: step one focuses on the theory of both business continuity management and IT governance whereas step two focuses on specific instances of IT governance frameworks. The aim of the literature survey is to analyse the viewpoints of authors to gain an understanding on the research topic and to formulate conclusions on the research objectives.

The first step of the literature survey focuses on the concepts of business continuity management and IT governance on a high conceptual level. Step one's literature survey on IT governance is dedicated to the theory of IT governance and not on IT governance frameworks. Complementing the literature survey on IT governance is the literature survey on business

continuity management. This literature survey focuses on material related to business continuity management and the conclusions derived from this survey form the basis of the empirical study.

Step two of the literature survey is dedicated to the investigation of IT governance frameworks with the specific goal of identifying how they contribute towards business continuity management. Specifically, the COBIT and ITIL IT governance frameworks are studied. The literature survey on these frameworks focuses on the continuity processes they offer. The results of the literature survey's step two are used to conduct the research method, namely the content analysis.

1.5.2.2 EMPIRICAL STUDY

The empirical component of the research approach consists of interviews. Specific practitioners were identified and based on relevant experience, expertise and positions within their respective organisations, invited to participate in the research. A prerequisite of all participants was for them to have a sufficient amount of knowledge in the area of business continuity management and IT governance. Both individuals and consultants, who are responsible for business continuity management and/or IT governance within their organisation or at client implementations, were considered for the interviews. The empirical study supplements the information derived from the literature survey in an attempt to gain a more comprehensive conceptualisation of business continuity management.

The interviews were semi-structured and based on the literature study (on both business continuity management and IT governance) completed in the first step of the research methodology. The interviews served as an opportunity to dynamically obtain knowledge and insights from the participants on the relevant research topics. By liaising with expert practitioners, information on the topic of business continuity management was identified that was not as explicit in the literature. A comparison between the practitioners' and literature's perspectives on business continuity

management indicated consistencies and inconsistencies between these two sources. The result of the interviews had a valuable contribution to the evident lack of academically oriented information on the topic of business continuity management.

1.5.3 METHOD

This research uses a specific method, namely content analysis. The content analysis examined the data obtained from the literature survey in a structured fashion. The result of the content analysis presented the researcher with information from which a business continuity management framework was developed. The text analysed in the content analysis was the official documentation of the IT governance frameworks namely COBIT and ITIL. The documentation focuses on the identification of processes to govern IT activities within an organisation, the scope of these processes and how the success of these processes should be measured. The content analysis analysed the IT governance processes dedicated to the continuity of an organisation. The motivation for conducting a content analysis on IT governance framework literature is to identify the underlying conceptualisations that IT governance has on business continuity management in a structured and organised manner. More on the theory of content analysis is presented in the chapter two, whereas the execution steps of the content analysis are documented in chapter five.

1.6 EXPECTED FINDINGS

The researcher expects some degree of difficulty during the first step of the literature survey, specifically the literature on business continuity management: As discussed in the problem statement, the researcher acknowledges the lack of and inconsistencies in the literature on business continuity management. The second step of the literature survey is expected to be unproblematic – a variety of sources exist on IT governance frameworks, albeit not all of sound academic value. It is expected that many of these IT governance frameworks have positivistic and deterministic flavours

attached to them. This might also become apparent through the empirical part of the research where the researcher expects a variety of perspectives on business continuity management. Lastly, the researcher is convinced that by examining IT governance frameworks, valuable information on business continuity management can be identified.

1.7 LIMITATIONS OF RESEARCH

A framework similar to the IT governance frameworks and the one developed in this research typically consists of different objectives that contribute to the goal of the framework. Each of these objectives has a set of detailed objectives associated with it, which subdivides the scope of the objective into manageable chunks. Each objective also has different managerial guidelines that define its relationship with other objectives, a RACI chart (responsible, accountable, consulted and informed) detailing the roles and responsibilities associated with the objective, goals, and metrics and maturity models.

The scope of this research is limited to defining the objectives, detailed objectives and RACI chart for a general business continuity management framework. The purpose of this research is to initiate the development of such a framework. However, the framework developed in this research is limited in scope and does not include sections focussing on the goals, metrics and maturity models of each objective. It is also acknowledged that the framework developed in this research does not satisfy all the business continuity management requirements of practitioners – after all, there will never be a 'one-size-fits-all' approach to business continuity management (Graham & Kaye, 2006:10). Nevertheless, the result of this research should be valuable to both academics and practitioners alike.

1.8 CONTRIBUTION TO THE FIELD OF INFORMATION SYSTEMS

In recent years, both business continuity management and IT governance have gained tremendous popularity with organisations. The success of most modern organisations is fundamentally dependent on its IT infrastructure and

its alignment with business objectives (Van Grembergen, 2003:242; Weill & Ross, 2003:1). Equally important is the assurance of an organisation's continuity regardless of a disaster, attack or malicious event. The importance of these managerial initiatives is emphasised by the examples presented in the beginning of this chapter. Without a theoretical basis for business continuity management, academics might fail to completely understand and improve the continuity of Information Systems. The lack of an academic basis for the research topic might cause practitioners to fail in the development and implementation of a sound and comprehensive business continuity management framework.

Evidently, the research might be valuable to both academics and practitioners in Information Systems. From an academic perspective, this research aims to initiate the development of a generally accepted business continuity management framework. This framework might also be valuable to executive practitioners like chief executive officers (CEO), chief information officers (CIO) and chief risk officer (CRO). Furthermore, the academic perceptions presented in this research might influence current managerial practices, or even initiate future practices. The conclusion of the research also provides practitioners with insightful literature propagating the latest academic perceptions and suggestions on the research topic in the field of Information Systems.

1.9 STRUCTURE OF THE RESEARCH

The following section presents a summary of the chapters included in this research:

Chapter 1 – Chapter one serves as an introduction to the research. It primarily focuses on the research details, including the problem statement; research objectives; and a section describing the importance of this research to the field of Information Systems. Chapter one also presents the hierarchical approach of the research, which consists of a paradigm, methodology and method.

Chapter 2 – The theory of Content Analysis. Chapter two presents a background on the theory of content analysis, which includes the content analysis execution framework used during this research.

Chapter 3 – An IT governance overview. This chapter describes and defines IT governance, the benefits it offers and presents a high-level overview and comparison of the most popular IT governance frameworks.

Chapter 4 – IT governance and business continuity management. Chapter four focuses on the evolution of IT governance and business continuity management together with the relationship between the two. The chapter also presents practices of IT governance frameworks that are dedicated to the continuity of an organisation.

Chapter 5 – Content analysis execution. The different execution steps of the content analysis method are detailed in chapter five, from the tool selection process to the validation of the results derived from the analysis.

Chapter 6 – Content analysis interpretation. Chapter six presents the interpretation of the content analysis's results. This includes the definition of business continuity management, the detailed objectives of business continuity management, the typical organisational role players responsible for business continuity management and the relationship that business continuity management has with the different IT governance frameworks.

Chapter 7 – Empirical study details and findings. The interviews with different practitioners focused on the objective of business continuity management and IT governance, the relationship between business continuity management and IT governance and the level of integration between the two areas. The chapter also explores the key role players responsible for business continuity management, the main challenges of business continuity management and the detailed objectives within a typical business continuity management framework.

Chapter 8 – A framework for business continuity management. The business continuity management framework that was formulated based on the results of the literature survey, content analysis and empirical study, is presented in this chapter. The main challenge associated with business continuity management is also be explored.

Chapter 9 – Conclusions, recommendations and future research. The final chapter presents a summary of the various topics presented throughout the research. In conclusion, recommendations to practitioners for executing business continuity management successfully are suggested. Future research topics will also be proposed for academics.

Glossary: A list of abbreviations used and their meaning.

References: Publications referenced in the research.

1.10 CONCLUSION

The importance of business continuity management has become evident after the occurrence of natural disasters, attacks and malicious events in recent years. The continuity of most modern organisations has become fundamentally dependant on the organisation's IT infrastructure. The assurance of the availability of an organisation's IT infrastructure is one of the objectives of IT governance. IT governance has become an integral part of the managerial responsibilities which executives have to ensure the efficient and effective delivery of IT benefits. The goal of this research is to develop a strong theoretical framework for business continuity management by using IT governance as a frame of reference.

CHAPTER 2
THE THEORY OF CONTENT ANALYSIS

2.1 INTRODUCTION

The content analysis research method is one part of the research approach. Content analysis is a structured way of processing text, amongst others. The goal of this chapter is to present the theory of content analysis prior to the execution thereof. A substantial part of this chapter is devoted to defining and explaining the content analysis framework utilised in this research. The execution steps of the content analysis framework are presented in chapter five.

2.2 DEFINING CONTENT ANALYSIS

Carley (1993:75) describes content analysis as the procedures for coding and interpreting text, amongst others, through the extraction of concepts within the text. According to Krippendorff (2004:19) content analysis is based on the interpretation of text and should be both reliable and valid. Schultz (1959:503) also recognises the importance of reliability and validity when conducting content analysis and defines content analysis as the transformation of text into meaningful information. Neuendorf (2002:112) also elaborates on the reliability and validity of content analysis. The reliability of content analysis is the successfulness which other academics can repeat the analysis and achieve similar results. A content analysis is not successful if it cannot yield the similar results when repeated by other individuals. The validity of a content analysis is determined by the extent to which the conclusions derived can withstand criticism and whether the correct measures were used to satisfy the research objectives.

Krippendorff (2004:22) describes six characteristics of text that are typically analysed through content analysis:

- The text itself has no goal without reader interaction;

- The text consists of multiple meanings as interpreted by the reader;
- The messages derived from text is unique and not necessarily shared;
- The reader's conceptualisation of text is much more than just the text itself – it includes feelings; and
- The conclusions derived are relevant to the context of the selected text.

Originally, the objective of content analysis was mainly of a quantitative nature. However, the next section explains the qualitative attributes of modern content analysis.

2.3 QUALITATIVE AND INTERPRETIVE NATURE OF CONTENT ANALYSIS

Content analysis is often regarded as being a positivistic (Neuendorf, 2002:11) and a quantitative method (Neuendorf, 2002:1) to analyse text. The statement is motivated by the argument that content analysis typically presents numeric summaries of the analysed text Neuendorf (2002:14), often derived from statistical calculations and validations. However, the introduction of qualitative and interpretive content analysis was introduced as early as the 1950's by Kracauer (1953:631) and Schultz (1959:503). Despite this, Krippendorff (2002:15) mentions that the majority of traditional content analysis studies were positivistic and quantitative of nature. Modern research has proven the value of qualitative content analysis research, which often utilises computer based text analysis. Roberts (1989:147) also recognises the two approaches (quantitative and qualitative) of conducting content analysis and explains that both approaches have its shortcomings and virtues. Yet, according to Kracauer (1953:637) these two approaches are 'not radically different approaches'.

Krppendorff (2002:16) argues against the proposition that content analysis is limited to a positivistic quantitative approach. Qualitative text can also be

analysed and often the results of a content analysis should be interpreted in an emancipatory fashion, resulting in the research being interpretive. This view is also supported by Kracauer (1953:631). The following list explains why content analysis can follow a qualitative approach:

- The interpretative nature of content analysis motivates users to process specific texts repeatedly through the continuous contextualisation and interpretation of different texts. Often this repetitive process is followed when researchers use hermeneutic circles to interpret the given text. When using a software tool, the researcher should analyse text using the Key Word In Context (KWIC) approach to ensure that the text is interpreted in the correct manner (Krippendorff, 2004:17; Roberts,1989:148);

- The different components of content analysis need not be executed in a sequential order. Often, through the interpretation of the text, the researcher needs to fall back to previous interpretations. By following a qualitative analysis, the researcher is able to conduct each component in a manageable way (Krippendorff, 2004:87);

- Typically, qualitative content analysis provides more accurate results compared to quantitative analysis (Kracauer,1953:631);

- Qualitative content analysis caters for different interpretations, perceptions and opinions through the utilisation of multiple text sources (Krippendorff, 2004:87);

- Qualitative content analysis makes provision for extreme cases whereas quantitative content analysis often disregards these cases (Kracauer, 1953:636);

- Interpretations of qualitative content analysis can be supported through the quotation of supporting text (Krippendorff, 2004:87); and

- Qualitative content analysis focuses on the detailed processing of a limited amount of text about a specific area of interest (Krippendorff, 2004:17).

2.4 CONTENT ANALYSIS FRAMEWORK

The content analysis framework executed in this research is aligned with the qualitative and interpretive framework proposed by Krippendorff (2004:29). The different steps of the framework are now discussed in sequential order, as presented in Table 1. These steps are followed during the execution of the content analysis, as presented in chapter five.

Table 1: Execution steps of the Content Analysis Framework

Step	Description
1.	Identification of research objectives and specifically the research questions. If organised text is analysed without a research question, the exercise becomes exploratory as to expeditiously.
2.	Identify unorganised text that might support the research objectives. Recognise various text sources and formats that might contribute to the different research questions.
3.	Step three is known as data making. Identify and understand (interpretive) the source and context of the text analysed as to avoid ambiguity. This step converts the unorganised text to organised text that is be used during the analysis.
4.	Analyse the organised text using a specific approach. During the analysis of the text, the different components of content analysis should be executed but not necessarily in sequential order. These components are presented Figure 4**.**
5.	Interpret the results of the analysis and derive conclusions from the analysis.
6.	Validate results. According to the definition of content analysis, researchers should ensure that the results are both reliable and valid. Note that by successfully repeating a content analysis merely indicates that the exercise is reliable and not necessarily valid (Krippendorff, 2004:40). Conclusions derived from the organised text needs to be validated against the unorganised data.

The reliability of a content analysis study can be enhanced, according to Krippendorff (2004:217), in the following manner:

- Step by step documentation of the entire analysis, including motivation for each decision made;

- Should there be more than one observer, the selection criteria for observers should be specified together with the required training to ensure consistency throughout the research; and

- Observers should work independently of each other as to not interfere with the individual interpretations. The research is only reliable when different observers acquire the same results independently.

The validity of a content analysis research is confirmed in the following manner:

- Face validity is when the research results are obvious and expected (Krippendorff, 2004:314; Neuendorf, 2002:115);

- Social validity is when the results of the research is accepted and appreciated by practitioners beyond the academic world (Krippendorff, 2004:314);

- Empirical validity is based on satisfactory evidence collected throughout the duration of the research (Krippendorff, 2004:315);

- Content validity identifies all attributes of the research objective and evaluates how accurate the analysis represents these attributes (Krippendorff, 2004:315; Neuendorf, 2002:116);

- Construct validity recognises other concepts in the social sciences and identifies how well the analysis compares against the constructs derived from these sciences (Krippendorff, 2004:315; Neuendorf, 2002:117); and

- Instrumental validity is when the results of the research are compared with correlating external measures (Krippendorff, 2004:315).

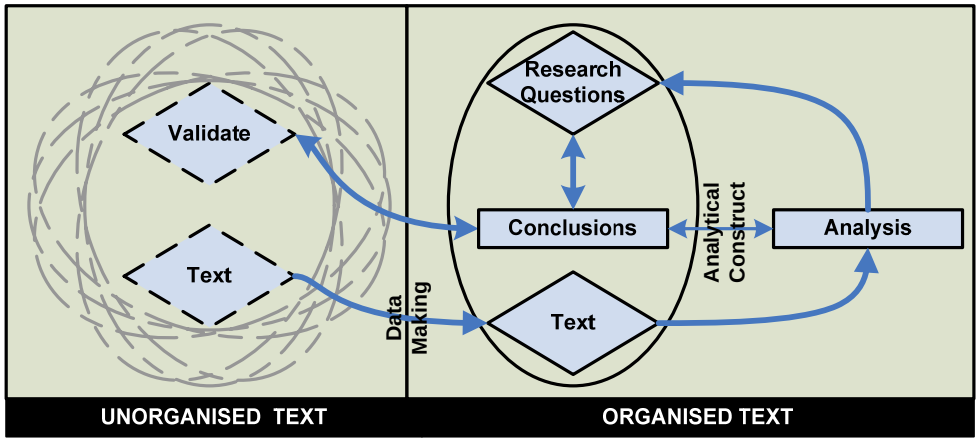

Figure 3: Content Analysis Approach – Adopted from Krippendorff (2004:30)

Unorganised text that is used in a content analysis refers to the raw and unprocessed text. Step one identifies the different unorganised text that is applicable to the research objectives. Step six makes use of the same unorganised text to validate whether the conclusions derived from the content analysis are consistent with the text.

Organised text refers to the unorganised text that contributes towards the research objectives and that has undergone categorisation, filtering or limited processing prior to the actual analysis. Steps three's transition of unorganised text into organised text (Figure 3) is referred to by Krippendorff (2004:83) as data making. From the organised text the actual analysis is performed, as indicated in step four. Step five attempts to draw conclusions through the creation of analytical constructs based on analysis and research objectives.

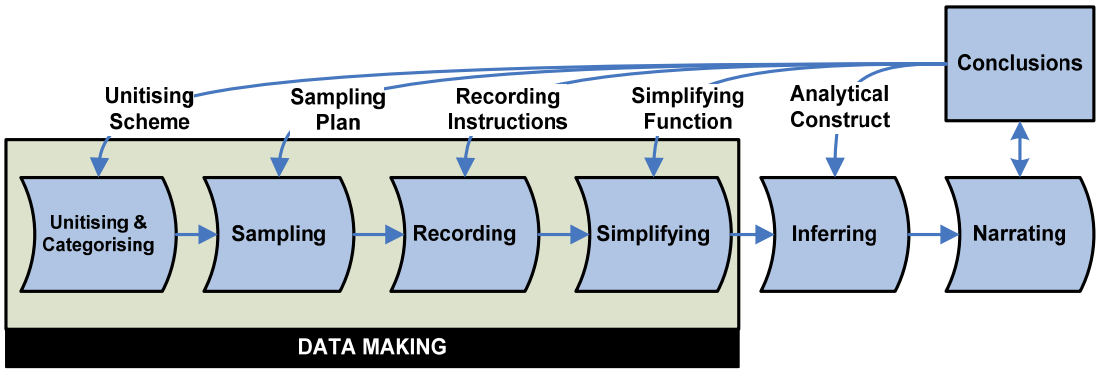

Figure 4: Content Analysis Components - Adopted from Krippendorff (2004:86)

Data making consists of a few components as illustrated in Figure 4. A description of these components and some additional content analysis components are now described:

- Unitising is the segmentation of text into appropriate units that are used during the analysis. Neuendorf (2002:13) mentions that the unitising approach is mostly consistent for different unit types but it can also differ. Typically, units can be of type 'words', 'sentences' and 'paragraphs' but it can also be more abstract like 'time periods', 'sounds', 'length', etc. Each unit type must be assigned to a unit category. Examples of different unit categories are, according to Krippendorff, (2004:99):

    - 'Sampling' units are units specifically selected from a larger population, according to the researcher's interest, goal or convenience;

    - 'Recording' units are created whenever the presentation or conceptualisation of the analysed texts, are not in a consistent format; and

    - 'Context' units are created by extracting information from existing sources and categorising it in a manner relevant to the research objectives.

- Sampling typically evaluates each unit and identifies a smaller set of units that are statistically representative of all units. In qualitative content analysis, sampling does not follow a statistical approach. Instead, quotes from the unorganised text are presented to motivate conclusions (Krippendorff, 2004:84). Also, in qualitative content analysis the process of defining the sample size is not applied in the same way as in quantitative content analysis. Instead, qualitative content analysis rather selects samples according to their relevance and contribution to the research objectives. The different techniques of

sampling are categorised according to random sampling and non-random sampling.

- Random sampling is the process of selecting different units, each with equal probability, according to no predefined specification (Krippendorff, 2004:114; Neuendorf, 2002:83). The different types of random sampling are:
  - Simple random sampling selects units using no statistical approach (Neuendorf, 2002:83);
  - Systematic sampling is when units are selected according to a predefined interval with a random starting point (Krippendorff, 2004:115; Neuendorf, 2002:83);
  - Cluster sampling is when the different units are grouped into clusters and then analysed as a whole (Krippendorff, 2004:116; Neuendorf, 2002:85);
  - Stratified sampling makes use of other sampling techniques but select only one per defined stratum (Krippendorff, 2004:115; Neuendorf, 2002:85); and
  - Multistage sampling consists of a combination of other random sampling techniques.
- Non-random sampling is when the unit selection process follows a statistical approach. Neuendorf (2002:87) argues that non-random sampling should only be used when it is not feasible to follow a random approach. Different non-random sampling techniques are now presented:
  - 'Varying probability' sampling is when each unit is prioritised according to the likelihood of the unit's source

contributing to the research objectives (Krippendorff, 2004:116; Neuendorf, 2002:88);

- ‘Relevance/purpose’ sampling is when the researcher prioritises each unit according to the unit’s contribution to the research objectives (Krippendorff, 2004:118; Neuendorf, 2002:88);

- ‘Snowball’ sampling is when the research starts with a given set of sample units to which extra units are added according to a specific criteria (Krippendorff, 2004:117);

- ‘Census’ is when all units identified in the research are included in the sampling (Krippendorff, 2004:120); and

- ‘Convenience’ sampling is when the researcher is not interested in applying a specific technique to identify the sample set, but rather include units based on predefined knowledge about how the unit contributes to the research objectives (Krippendorff, 2004:120; Neuendorf, 2002:87).

- Recording is the process of creating repeatable representations of abstract objects to have a consistent basis to perform the analysis on. One such example is an image. People are likely to interpret an image in different ways. Recording attempts to record a particular interpretation (in either text or audio) to make it consistent for the sequential steps of the analyses. Krippendorff (2004:84) points out that written text is already recorded as the text itself is presented to different people in a consistent manner.

- The simplifying of text attempts to modify the text as to improve the processing of the text. Carley (1993:83) makes a valid suggestion: different text versions should be stored during the text simplification activities. This is because often, after the text has been analysed,

interpretations of the text cannot be concluded as the text is not in a grammatical format anymore. Text reduction includes activities like the removal of duplicate text sources. When using a software tool to conduct qualitative analysis, Krippendorff (2004:282) suggests that the following activities are completed to reduce the volume of text:

- Text cleansing attempts to remove unwanted units from the text source. This includes the replacement of illegal characters so that all text can be interpreted by the software; the correction of spelling mistakes and the transformation of characters into a unified case, should the software be case sensitive;

- The categorisation of text attempts to identify sections within the text that might be helpful during the content analysis. Typical activities include using specified names as pronouns and/or indirect references; specifying the contextual function of the word e.g. whether it is a noun or verb; specifying the analytical category of the text e.g. description, validation or justification; clarifying homonyms (especially applicable when interviews are translated to text); and specifying markers within the text so that the software can identify distinctive sections within the text e.g. introduction, conclusion or summary;

- Modifying text is about changing the text according to requirements of content analysis with the goal of improving the results. Typically, this includes the removal of units that does not contribute towards the research objectives; compact the text as to reduce redundant units; and reformatting of the text as to unwrap the key messages and disregard the 'packaging' e.g. the removal of page numbers; and

- Specific packaging of the text is needed in cases where a software tool is used. The packaging then transforms the text according to the software tool requirements.

- Inferring refers to the analysis of the text and the conclusions derived from the analysis. The analysis focuses on the meaning of the text, to what the text refers to, what it entails, provokes and any unobserved phenomena's. Often during the inferring process, the researcher makes use of a software tool. Krippendorff (2004:262) describes the different categories of motivations as to why software tools should be used:

    - Partition of text into desired units e.g. words, paragraphs or concepts;

    - Text searches to identify valid text sources;

    - Transformation of text into visual representations to simplify the interpretation thereof; and

    - Interactive hermeneutic approaches that allows the researcher to develop coding sections.

  When executing the inferring component, different analytical techniques can be used to perform the actual analysis. Most of these techniques are executed within the help of a software tool and examples of these techniques are as follows:

    - Frequency analysis is the most often used by content analysis research. This technique performs a count on the distinct units presented according to the specified categories. This can be done through absolute frequencies, where the number of occurrences of each unit is identified, or relative frequencies where the unit occurrences number is calculated as a percentage of the total number of units. The motivation for executing a frequency analysis to identify key words within the text. This technique is based on the assumption that the more

often a word appears in a given text, the more likely the text is about the concept which the unit represents;

- Association analysis makes use of variables that represents relationships between different units. The variables can be defined by the researcher but typically this analysis type is most effectively used when the research has predefined variables and a criterion test that must be performed;

- Contingency analysis extends the frequency analysis and attempts to identify co-occurrences between units in different categories. Contingency analysis argues that the perceptions derived from the text (based on individual interpretation) should be supported by the statistical calculation of units and the relationship between these units;

- Clustering attempts to reduce the number of variables or unit groups based on the grouping of variables/groups according to similar characteristics; and

- Quotes and unit analysis. A big part of interpretive content analysis is the identification of quotes and the assignment of quotes to units. Quotes are based on the units declared for the analysis and can be single units, or a combination of units. Each quote is linked to a code that is used to motivate the conclusions derived from the analysis.

- The final component is the process of narrating the results of the analysis according to the research questions. Typically this includes an explanation of the significance of the research, implications it might have to the audience and the contribution it has to possible future research.

2.5 CONCLUSION

Content analysis is a research method that analyses text in a structured manner. The result of a content analysis derives information from text that is relevant to the defined research objectives, in a specific format. Specifically, this chapter discussed the theory of the content analysis framework executed in this research. The execution steps of the framework are detailed in chapter five, whereas the interpretation of the results obtained from the execution is presented in chapter six.

CHAPTER 3
AN IT GOVERNANCE OVERVIEW

3.1 INTRODUCTION

The need for effective and efficient management of IT investments has become compulsory to ensure the achievement of business objectives. Consequently, IT governance was developed and has since become an essential managerial activity for most modern organisations. Practitioners now have the option of implementing different predefined IT governance frameworks that follow industry standards, are auditable and easily acquirable.

In this chapter an overview of the different aspects of IT governance is presented. The following secondary research questions are answered:

- What is the definition of IT governance?
- What are the advantages IT governance claims to offer?
- What IT governance frameworks exist and how do they compare with each other?

3.2 DEFINING IT GOVERNANCE

The majority of modern organisations have become fundamentally dependant on IT to perform their daily operations (Weill & Ross, 2003:1; Calderon & Dishovska, 2005:21). IT has become such a business enabler that organisations motivate their IT expenditures as investments that contribute towards the continuity of the organisation. As Carroll *et al.* (2004: 233) mentioned, large organisations' annual capital investments on IT can contribute as much as 50% of the total expenditures made by the organisation. This is supported by Sohal & Fitzpatrick (2002: 101) who are convinced that IT is one of the top expenditures an organisation can have.

However, according to Kan (2003: 2) these IT expenses can be justified and should rather be seen as investments as it is contribute towards the sustainability of an organisation's success. This implies that IT governance can contribute towards an organisation's business continuity.

The primary goal of IT governance is to align an organisation's information technology with its business (Parker *et al.*, 2002:3143). The design of an organisation's IT and business strategies need to be aligned with the corporate strategy in an attempt to ensure accurate IT governance initiatives (Parker *et al.*, 2002: 3143; Schwarz & Hirscheim, 2003: 131). The success of a corporate strategy relies on how an organisation embraces IT in the business environment (Exler, 2003). However, IT should always be regarded as a business enabler and not as the business itself (Elliott *et al.*, 1999:43). This characteristic defines IT governance as the integration of business and IT (Parker *et al.*, 2002: 3143) to ensure that IT operations are aligned with business objectives. The consequence is for IT investments to deliver more business value (Patel, 2002: 3167). Much emphasis is placed on how IT governance allows business value to be leveraged from IT investments. IT governance also aims to prioritise and often restrain IT expenditures in an attempt to discipline IT related costs (Hoffman, 2003: 14).

The alignment of business objectives and IT operations are often more problematic than expected (Burn & Szeto, 1999: 197): IT governance can only successfully deliver business value from IT investments when it is implemented across all organisational units. This is supported by Burn & Szeto (1999: 197) who motivate that IT governance is based on the 'lateral decision-making processes' between the business and the IT divisions. However, the successful implementation of IT governance across the entire organisation does not guarantee perfection. Additionally, all organisational units must be consistent in their IT governance implementations (Koch, 2002). A major factor ensuring a successful enterprise IT governance implementation is the ownership of the initiatives and the disciplined execution thereof. The ownership of IT governance in an organisation is considered to be the limited decision-making structures (Weill & Ross, 2004) developed from a hierarchy

of defined roles and responsibilities (Schwarz & Hirschheim, 2003: 148). For this reason IT governance is seen as a managerial activity (Kan, 2003:2) specifically assigned to the directors, executives and IT managers of the organisation (Van Grembergen, 2003: 242). Patel (2002:3163) is convinced that IT governance, being a managerial activity, improves the accountability of IT related functions in the organisation. This also increases the quality of an organisation's products and/or services as more IT opportunities are embraced, resulting in higher return on investment.

Higher return on IT investments can also be achieved by ensuring the delivery of expected IT benefits, which is yet another characteristic of IT governance (Kan, 2003: 2). Weill & Ross (2004) agree and state that the delivery of expected IT benefits can only materialise if an organisation's executives can manage desirable IT behaviour.

The final characteristic of IT governance is highlighted by the IT Governance Institute (2000): IT governance aims to deliver successful IT initiatives whilst balancing risks. As a result of the exponential developments in the field of technology, the acquisition of this technology is often accompanied by risks. Even though the latest technology can be extremely beneficial to an organisation, history has proven that the aging of some of these technologies can be to the expense of an organisation when it does not become an industry standard. This is one example used to illustrate the strong relationship between IT governance and risk management.

IT governance is defined as:

> *IT governance is a framework of IT-related processes that is aligned with business strategy and focused on the delivery of maximum IT value from disciplined IT investments, while balancing risks.*

The two most popular IT governance frameworks are COBIT and ITIL (Carroll *et al.,* 2004: 233). Both these frameworks are internationally utilised and have received much acclaim over the last couple of years. Although COBIT and

ITIL have been accepted as IT governance frameworks, it is important to note that these two frameworks share a limited, if any, amount of functionality and scope. COBIT focuses on the alignment of an organisation's IT goals with the different business objectives in an organisation (Carroll *et al.*, 2004:233). The ITIL framework on the other hand, is a set of best practices for an organisation's IT processes and is regarded by Kim (2003:13) as the most popular framework for the management of IT. Each framework has its own strengths and weaknesses and many practitioners will argue forcefully to the favour of either of the frameworks. Many organisations adopt a hybrid between COBIT and ITIL to create a comprehensive and unique IT governance framework. More on these frameworks is presented later in this chapter.

3.3 BEFITS OF IT GOVERNANCE

IT governance claims to deliver a large amount of benefits if implemented properly by an organisation. These benefits are not related to only IT. The following section is a limited list of benefits which IT governance claims to deliver, as proposed by the literature:

- Best practices of IT functions (Kim, 2003:13). IT governance (with specific reference to the ITIL framework) is dedicated to a list of IT related best practices. An organisation merely needs to customise and implement these best practices;

- Prioritisation of IT initiatives (Hoffman, 2004:6). Either an organisation's business department or the IT department can initiate new IT projects. IT governance aligns the various IT requests and prioritise them according to their contribution to business strategy and the delivery of business value;

- Clearly defined IT related roles and responsibilities (Hwang & Liu, 2003:11). IT governance facilitates the allocation of organisational

resources to IT processes together with clearly defined tasks that they are held accountable for;

- Effective and efficient IT management (Schwarz & Hirscheim, 2003: 129; Van Grembergen, 2003:242; Hwang & Liu, 2003:13). IT governance assists executives to steer IT initiatives into a clearly defined and unified direction;

- Proper IT standards (Hwang & Liu, 2003:13). IT standards are critical to the sustainability and quality of IT operations. Often IT governance frameworks are supplemented with the standards as prescribed by the International Standards Organisation (ISO);

- Improved product and/or service quality (Patel, 2002:3163). By having an IT governance framework, an organisation's IT delivery should be of high standard. A sound IT infrastructure should provide an organisation with a proper backbone to complete the daily business operations;

- Increased organisational value and success (Hwang, 2002:15; Kan 2003: 2). The increased value delivery by an organisation eventually results in the improvement of organisational success. One of the goals of IT governance is to ensure the delivery IT value, hence contributing to the success of the organisation;

- Shareholders satisfaction (Parker *et al*., 2002:3143). The satisfaction of shareholders should improve as an organisation's IT governance framework matures and the performance of the organisation improves;

- Disciplined IT related costs (Hoffman, 2004:6; Patel, 2002:3163). IT governance ensures the central, unified and consistent management of an organisation's IT operations which decreases unnecessary IT costs;

- Return on investment (Patel, 2002:3163). An IT governance framework needs to mature and be maintained over a period of time before organisations can reap the full benefits of the implementation;

- Competitive advantage (Patel, 2002:3163; Dahlberg & Kivijarvi, 2006:194b). By cutting IT related costs, enabling more efficient IT processes and improving product and service quality, IT governance allows organisations to outperform competitors who have not implemented an IT governance framework;

- Decreased IT related risks (Carroll *et al*., 2004:233). As IT governance aims to align IT functions with business operations, the purpose and scope of the IT functions are accurately controlled, resulting in the decrease of IT related risks;

- Assurance of IT benefits (Kan, 2003:1). As a result of IT acting as an enabler of business processes, it is imperative that the expected IT benefits of the framework investment materialises. This is one of the main goals of IT governance; and

- IT and business strategy alignment (Parker *et al*., 2002:3143). According to the literature, this is the most important motivation for organisations to implement IT governance. All IT functions in an organisation should be aimed at supporting specific operations. Should IT be unsuccessful in doing so, IT is not likely to deliver any tangible business value.

These examples illustrate some of the benefits associated with the efficient and effective governance of IT. Some of these examples contribute strongly towards the definition and objective of IT governance such as the decrease of IT related risk and alignment between IT and business.

3.4 IT GOVERNANCE FRAMEWORKS

Even though IT governance implementations are mostly unique to each organisation, predefined frameworks such as COBIT and ITIL provide excellent generic guidelines. These guidelines can be utilised by organisations to serve as a basis for the development of an IT governance framework unique to them (Dahlberg & Kivijarvi, 2006:194b). This is supported by Anthes (2004:41) who also states that even though IT governance frameworks are customisable by organisations, all implementations ultimately have the same common goal: To improve the delivery of maximum IT value and benefits by ensuring the effectiveness and efficiency of IT operations. IT governance frameworks such as COBIT and ITIL are not mutually exclusive. Often organisations integrate different aspects of each framework to create a unique framework. As stated by Morency (2005:37), IT governance frameworks should rather be regarded as complimentary to each other than competitive. These IT governance frameworks can be integrated with existing business processes, an approach which is often followed when implementing ITIL in different phases (Cox, 2004:60).

This section presents a high level overview of the COBIT and ITIL IT governance frameworks, together with the advantages and disadvantages of each framework.

3.4.1 COBIT

The Control Objectives for Information and Related Technology (COBIT) is a framework jointly developed by the Information Systems Audit and Control Association (ICASA) and the IT Governance Institute (ITC). COBIT is currently in its fourth version which is also the version used by the researcher throughout the research. The scope of the COBIT framework is not limited to IT – COBIT's main emphasises is on the business of an organisation (Lainhart, 2001:19). COBIT focuses on the IT processes across the entire organisation, from the definition and implementation to the measurement, improvement and ultimately the auditing of the different processes (Morency, 2005:37). The goal of COBIT is to manage calculated IT risks through

defined and auditable internal controls. COBIT provides users with a comprehensive checklist to ensure the end-to-end control of critical business processes. Shareholders and customers can be assured of the credibility of these processes by the strong audit focused characteristic of COBIT (Lainhart, 2001:19).

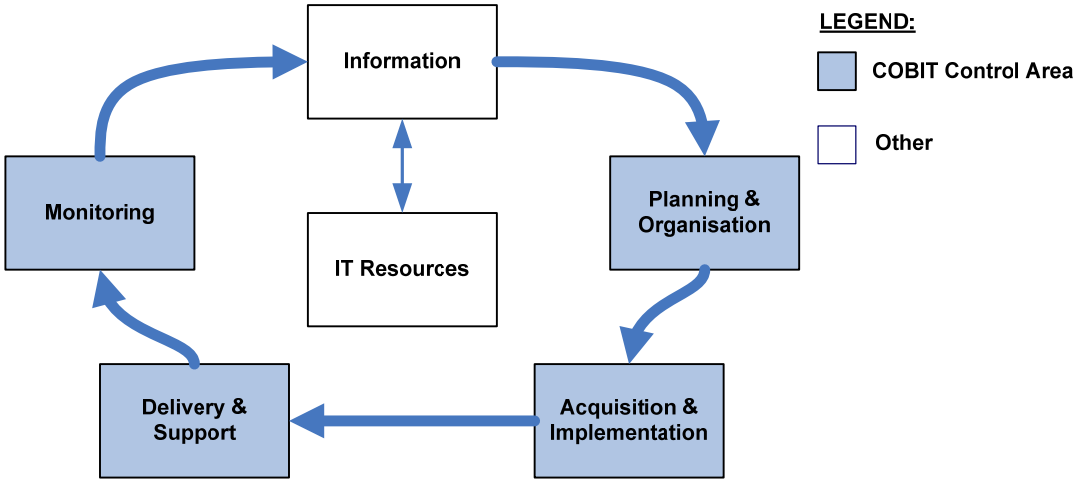

Figure 5: The COBIT Framework – Adopted from IT Governance Institute (2005:24)

The COBIT framework is presented in Figure 5. COBIT describes 34 high-level control objectives that are assigned to four main control areas (Anthes, 2004:43; Lainhart, 2001:19) namely:

- Planning and organisation: This control area includes the formulation of an approach, strategy and tactics aimed at utilising IT to ensure the delivery of business objectives;

- Acquisition and implementation: This control area focuses on identifying improvements, challenges and opportunities of how IT can be utilised to improve business process. The integration with legacy systems is also included in this step;

- Delivery and support: Delivery and support area is dedicated to making IT processes available to employees and customers. Additionally, this

category also ensures the effective support of the delivered processes; and

- Monitoring: The final control area is dedicated to the observation of IT processes to ensure that IT still meets quality standards and exceed compliance requirements. Monitoring should be conducted on regular intervals by means of internal audits. External audits should be conducted by independent auditors and should be executed less frequently (at least annually).

The complete COBIT framework consists of seven different components that discuss each of the COBIT control areas. The different COBIT components are published in both book and electronic format and are displayed in Figure 6.

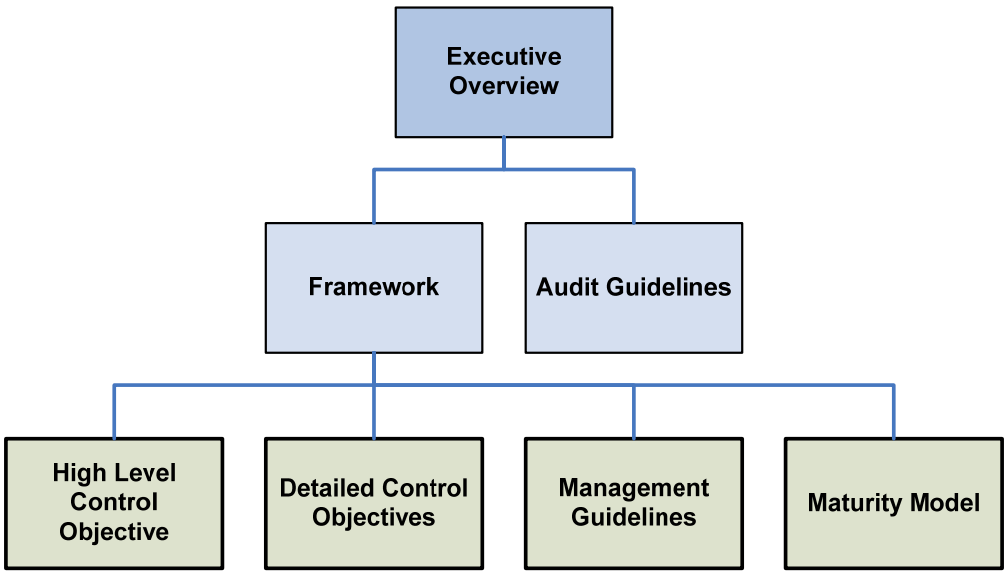

Figure 6: COBIT Components

The Executive Overview component details a high level overview of the motivation and advantages for implementing COBIT. Internal and external auditors to validate the execution of the processes mainly use the Audit Guidelines components. The Framework component consists of four subcomponents. The High Level Control Objective component explains the different control objectives and their relevance to the organisational resources. The Detailed Control Objectives component lists the in-depth

control objectives to be implemented by the organisation to ensure the success of the high level control objective. Each category and the control objectives are discussed by means of four guidelines as detailed in the Management Guidelines product. Lainhart (2001:19) summarises the relationship between these management guidelines best: 'Critical success factors (CSF) suggest what needs to be done based on the choices made in the maturity models, while monitoring through key performance indicators (KPI) whether the enterprise is likely to reach the IT process goal set by the key goal indicators (KGI)'. In more detail, the management guidelines are as follows (Anthes, 2004:43; Morency, 2005:37):

- Critical success factors (CSF's): Identifying criteria that are crucial to the successful implementation, execution and control of a control objective. Conditions can be strategic, technical, organisational or procedural;

- Key performance indicators (KPI): Measurements of each control objective and the summarisation of its performance. Each control objective is usually process based but IT driven; and

- Key goal indicators (KGO): Identification of accurate targets or outcomes that the objectives need to surpass, i.e. whether IT processes are achieving business goals. KGI's are mostly measured in terms of availability, risks, costs, reliability, effectiveness and compliance.

Lastly, the Maturity Model component analyses the organisation's implementation of each control objective to identify the level of maturity ranging from non-existent to optimised.

3.4.1.1 STRENGTHS OF COBIT

COBIT provides an audit-oriented set of comprehensive checklists specifically aimed at minimising IT related risks (Anthes, 2004:43). Should organisations

implement an IT governance framework for compliance reasons (like the Sarbanes-Oxley Act), the clear audit characteristics of COBIT make it the framework of choice (Morency, 2005:37). Additionally, COBIT's strong focus on corporate governance makes it the ideal framework for an enterprise wide implementation, hence the evident managerial characteristic provided by COBIT. The fact that COBIT is reasonably easily obtainable allows all types of organisations to effortlessly study and implement the COBIT framework.

3.4.1.2 WEAKNESSES OF COBIT

A limitation of the COBIT framework is the fact that it details only the high level control objectives which organisations need to implement and not the implementation process. Similar to ITIL, COBIT does not specifically discuss software development activities, nor provide a road map for continuous process improvement (Anthes, 2004:43). COBIT does not have such a strong focus on IT services when compared to ITIL, specifically on IT delivery and support.

3.4.2 ITIL

The UK Government initially developed the IT Infrastructure Library (ITIL) framework almost 20 years ago. New releases have since been updated by practitioners and distributed by the UK publisher The Stationary Office. Today, practitioners can consult various external companies like Pink Elephant to assist them in understanding and implementing ITIL. The ITIL framework has gained such popularity in recent years that individuals now have the opportunity to become ITIL certified. The ITIL version referenced in this research is version two.

By successfully implementing the complete ITIL framework, organisations can expect to decrease IT costs by 50% (Dube, 2004:1). However, organisations do not need to implement the entire ITIL framework to obtain some of the benefits offered by ITIL. Even by implementing only specific disciplines from the various ITIL sets, organisations can achieve tremendous value from the

best practices proposed by ITIL. Hochstein *et al.* (2005:704) object to ITIL being described as 'a best practice framework' and present arguments to support that (from an academic perspective) ITIL should rather be categorised as a common-practice framework. The motivation being that a best practice framework is formulated from innovative insights that are based on a well-founded theory, a characteristic that ITIL fails to emphasise. Regardless of this, practitioners all over the world have desperately grasped ITIL as an IT management guideline, yielding in evident success.

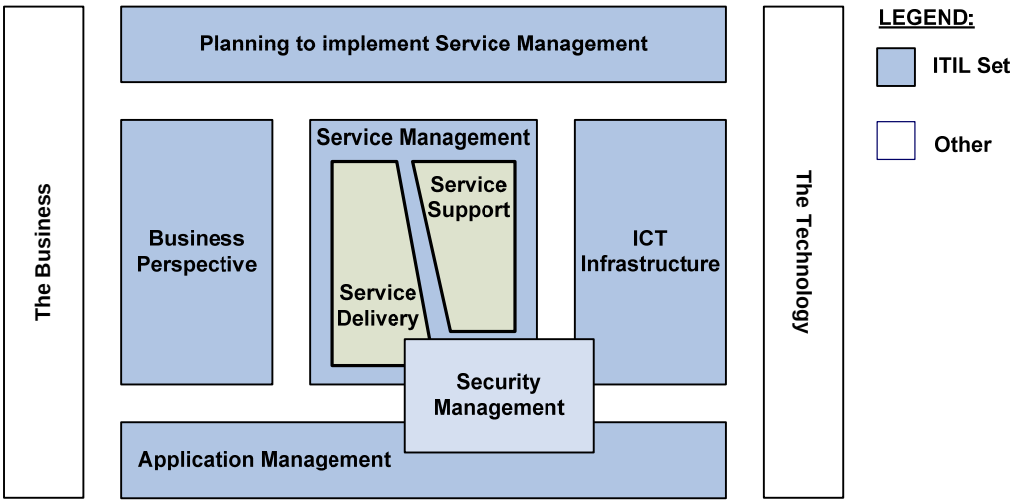

Figure 7: The ITIL framework – Adopted from Office of Government Commerce (2002a)

The ITIL framework consists of a collection of generic IT best practices. These best practices are categorised into seven sets (representative of seven books or CD's) and can be further dived into different process elements. The ITIL framework focuses on delivering business value from technological investments made by the organisation. As indicated in Figure 7, the ITIL framework is positioned between the business operations and technology investments. Central to all other ITIL sets is Service Management that forms the heart of the framework and is dedicated to the control and monitoring of IT services. Service Management itself is not an ITIL set but rather an abstraction of two different sets contributing to Service Management, namely Service Delivery and Service Support. Complementing Service Management is the other ITIL sets that are: Planning to implement Service Management, Business Perspective, ICT Infrastructure, Application Management and Security Management.

The seven sets that make up the ITIL framework are as follows (Worthen, 2005:1):

- Planning to implement Service Management: This set explains the challenging process of introducing IT governance (specifically ITIL) to an organisation together with the approach and steps of implementing it;

- Service Support: Service Support is the discipline of providing an organisation's customers with different services to access the various service deliveries;

- Service Delivery: Service Delivery is the services an organisation requires of internal and external providers internal that is needed to support the organisation's business operations;

- Security Management: Dedicated to all security related issues, security management ensures the secure delivery of all organisational services;

- ICT Infrastructure Management: This set has a strong technical focus on the communication and technology infrastructure needed to successfully practice Service Management;

- Application Management: Application Management focuses on the management lifecycle of applications contributing towards the information services, as provided by the organisation; and

- Business Perspective: The Business Perspective set is aimed at providing business users with insight and understanding about IT services and how it needs to be managed in order to deliver business value. It is also about measuring the efficiency and effectiveness of IT services together with the financial management of each service.

3.4.2.1 STRENGHTS OF ITIL

What differentiates ITIL from other IT governance frameworks is the detailed level focus it has on IT (Worthen, 2005:1; Anthes, 2004:41). ITIL has been adopted by countless organisations as a comprehensive framework that is dedicated to the success and sustainability of all IT related processes in an organisation. ITIL aims to continuously improve the quality, effectiveness and efficiency of IT processes (Morency, 2005:37). As a result of this, ITIL has developed a solid reputation as being the *de facto* framework of IT best practices when compared to other IT governance frameworks (Anthes, 2004:41). One of the true strengths of ITIL is its ability to establish a common vocabulary of IT related aspects in the organisation (Dube, 2004:1; Cox, 2004:60). ITIL aims to erase miscommunications and misunderstandings in an organisation by enabling different departments to refer to the same thing using predefined terminologies.

3.4.2.2 WEAKNESSES OF ITIL

ITIL is often conceptualised as a 'ready to implement' packaged solution that consists of guidelines which details a successful IT governance implementation. Instead, ITIL offers a guide of high-level best practices that organisations should adopt and customise according to their requirements (Worthen, 2005:1). Additionally, critics have often slashed ITIL for its ambiguity and the high level of interpretation required by practitioners to implement the proposed best practices (Anthes, 2004:41). The absence of quality management (Anthes, 2004:41) in ITIL is perceived as another important limitation of the framework. Instead, practitioners suggest that ITIL is complemented by standards like ISO 9000 and Six Sigma to ensure the quality of IT operations. Lastly, the fact that the ITIL library needs to be purchased does make the framework less accessible to practitioners when compared to COBIT.

3.5 CONCLUSION

This chapter presented a high level overview of IT governance. IT governance focuses on the alignment of IT activities with business objectives

without obscure IT expenditures or risks. If implemented correctly, IT governance claims to deliver a variety of benefits to the organisation. The majority of these benefits were presented and discussed, as propagated by the literature. COBIT and ITIL were identified as the two most popular IT governance frameworks that are implemented by practitioners. An overview of each framework, together with its advantages and limitations, were also discussed.

The next chapter leverages of chapter three and focuses on the evolution and relationship between IT governance and business continuity management. As a result, specific business continuity management practices in the COBIT and ITIL IT governance frameworks are also discussed.

CHAPTER 4
IT GOVERNANCE AND BUSINESS CONTINUITY MANAGEMENT

4.1 INTRODUCTION

IT governance is not only limited to the delivery of various IT related benefits and the alignment between IT and business processes. IT governance also aims to improve the continuity of organisations. Most modern organisations have become fundamentally dependant on their IT infrastructure as IT has become an enabler of critical business processes. This chapter explores the development of IT governance and business continuity management in recent years and the relationship that exists between them. In conclusion, the different IT governance frameworks presented in the previous chapter are analysed to identify the specific components that contribute towards business continuity management. In the subsequent chapters, these components are referenced and analysed with the goal of developing a business continuity management framework.

Chapter four answers the following secondary research questions:

- How has IT governance and business continuity management evolved in recent years?
- What is the relationship between IT governance and business continuity management?
- Which processes in IT governance frameworks contribute towards business continuity management?

4.2 EVOLUTION OF IT GOVERNANCE AND BUSINESS CONTINUITY MANAGEMENT

The introduction of IT in organisations has vastly improved the manner in which commerce is conducted. Historically the success of organisations was dependant on their ability to manage the logistical challenges in a human intensive environment. The introduction of IT focussing on critical areas such as enterprise resource planning (ERP), customer relationship management (CRM), supply chain management (SCM) and business intelligence (BI), amongst others, has drastically influenced all areas in organisations. This includes organisational infrastructure, business processes and managerial activities to new markets and business opportunities. In the early days of IT governance, organisations recognised the critical role of IT in their organisation. This consequently resulted in the establishment of the traditional view of IT governance. As the continuity of organisations was mainly dependant on IT, the scope of traditional business continuity management initiatives was also mainly IT focused.

The traditional view of IT governance soon became obsolete and inadequate (Schwarz & Hirscheim, 2003:130; Parker *et al.*, 2002:3143) as organisations realised that the value of IT is limited to it being the enabler of business processes and not the business itself. This evolution of IT governance introduced frameworks such as COBIT and ITIL to ensure the alignment between IT and business strategy.

Similarly, the evolution of business continuity management has recognised business processes as the most critical element to ensure the sustainability of an organisation. Figure 8 illustrates how, over time, the scope of IT in business continuity management has gradually decreased in caparison with the rest. This is a result of the exponential scope expansion of business continuity management, specifically with the realisation that business processes are the foremost critical component of business continuity management. Figure 9 indicates that event though the scope of IT within business continuity management has decreased compared to the rest, the importance of IT within business continuity management has increased. The motivation for this is because organisations have become increasingly dependant on IT.

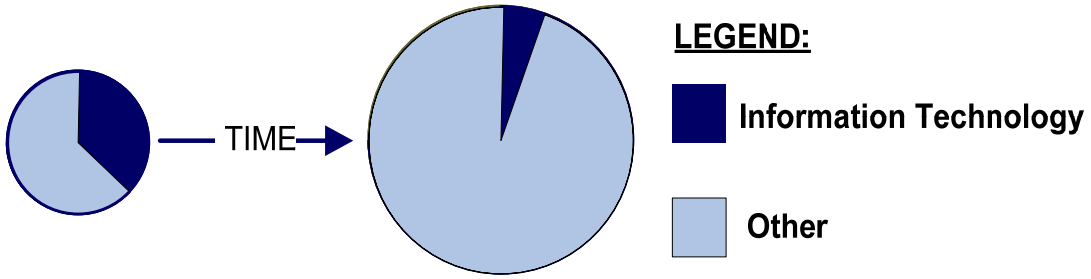

Figure 8: IT Scope within Business Continuity Management

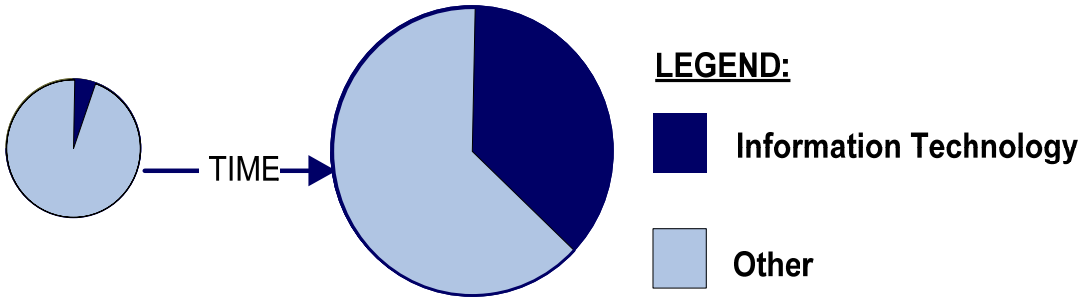

Figure 9: Business Continuity Management's Dependency on IT

This evolution of business continuity management and IT governance clearly indicates a paradigm shift in both areas. This paradigm shift is discussed in the sections to follow.

4.2.1 THE TRADITIONAL VIEW

Similar to business continuity management, the traditional scope of IT governance is described by Patel (2002:3166) as being limited to technology. This is confirmed by Schwarz & Hirscheim (2003:130) who explain that IT governance has traditionally focused on an organisation's IT infrastructure and the configuration thereof. Additionally, the impact that IT had in the business environment was limited to the organisation itself (Patel, 2002:3166). The traditional perspectives on IT governance did not cater for any external factors. The decision making structures presented in traditional IT governance frameworks are explained by Parker *et al.* (2002:3143) as being a hierarchical structure centralised and limited to the IT department. There was minimal intervention between business units and the IT departments. As a result of this, IT governance had a very static nature (Patel, 2002:3166), which resulted in IT silos in the different organisational departments. The traditional scope of IT governance is now considered to qualify as IT

management. However, the terminologies 'IT governance' and 'IT management' are still often used interchangeably and regarded as synonyms. As pointed out by Sohal & Fitzpatrick (2002:97), confusion is evident when differentiating IT governance from IT management. IT management is dedicated to the decision-making and functional work related to IT, whereas IT governance is more strategic of nature.

The traditional scope of business continuity management was limited to the IT functions in an organisation, as pointed out by Cummings (2005:S4). Elliott *et al.* (1999:43) support this statement and describe that traditional business continuity management failed to focus on the human related issues. The traditional business continuity management initiatives focused on creating backups of core systems and transporting it to secure sites, securing applications, storing data, ensuring a stable IT infrastructure, etc. Today, the traditional IT focused scope of business continuity management has been replaced with disaster recovery (Hiles & Barnes, 2001:67; Herbane *et al.*, 2004:435). However, IT still forms an integral part of business continuity management, as IT is critical to the sustainability of an organisation (Calderon & Dishovska, 2005:21). For this reason, disaster recovery is considered to be a subcomponent of business continuity management (Bakshi & Refeq, 2005; Rutherford *et al.*, 2002:4).

4.2.2 THE MODERN VIEW

Historically, organisations failed to recognise IT as the facilitator of business processes. The perspectives on the role of IT have matured to the realisation that the true value of an organisation is not a result of the technology used to conduct business activities, but rather the business processes itself. The role of IT adopted this evolution and was transformed from 'being' the business to 'supporting' the business.

In recent years, the role of IT governance has evolved from being mainly IT focused to realising the importance of business processes in the organisation. As presented by Schwarz & Hirscheim (2003:130), the modern perspective on

IT governance is much more than just technology: it incorporates both the strategic objectives set by an organisation and the environmental imperatives influencing an organisation. Patel (2002:3166) explains that the modern view on IT governance is to recognise the importance of business processes and then to align IT initiatives with these processes. By being business focused and not IT focused, IT governance can easily adopt new IT requirements that will result in a dynamic framework, as appose to a static framework (Patel, 2002:3166). Contributing to the dynamic nature of modern IT governance frameworks is the decentralisation of IT decision-making structures. These structures range across organisational units including corporate, business and IT departments. Each department should prevent the execution of managerial activities as exercised by traditional IT governance (it is the IT departments responsibility), but rather on the administration, coordination, appraisal and strategic planning of IT related activities (Sohal & Fitzpatrick, 2002:97). These departments are also in a better position to realise that modern IT governance is not limited to the organisation itself, but also includes customers, suppliers and business partners (Patel, 2002:3166).

Similarly, business continuity management has also matured from its traditional focus on IT and the IT department (Musaji, 2002; Cummings, 2005:s3). Similar to IT governance, the shift of IT's role in an organisation has resulted in the re-conceptualisation of the factors contributing towards the sustainability of an organisation. Calderon & Dishovska (2005:21) explain that business continuity management has evolved to a much broader concept that covers all aspects critical to the continuity of an organisation, of which IT is only one element. Resilient business processes replaced IT as the foremost important factor ensuring the continuity of an organisation. Consequently, the traditional scope of business continuity management became incomplete as it needed to be more comprehensive than just the traditional focus on IT (Cummings, 2005:S4). Hiles & Barnes (2001:26) agree and explain that the traditional focus was too narrow and not comprehensive enough to ensure the continuity of an organisation. Business continuity management evolved from having a technologically focused scope to being mainly business process oriented. The modern scope of business continuity

management focuses on business processes and the logic, skills and infrastructure needed to successfully support these processes (Musaji, 2002; Price, 2004:34).

4.3 THE RELATIONSHIP BETWEEN BUSINESS CONTINUITY MANAGEMENT AND IT GOVERNANCE

The relationship between business continuity management and IT governance is vital to ensure the continuous availability of an organisation's IT infrastructure. Certain IT governance initiatives should be guided by the business continuity requirements. This ensures that the necessary attention is given to business critical IT operations. Without the recognition of the relationship between business continuity management and IT governance, the comprehensiveness of the IT governance controls specifically focussing on the continuity of an organisation's IT infrastructure, cannot be determined. Figure 10 displays the relationship between IT governance and business continuity management.

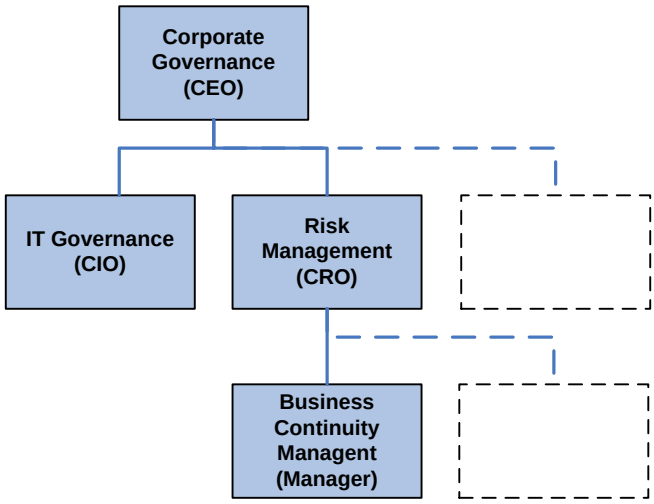

Figure 10: Relationship Between Business Continuity Management and IT Governance

Corporate governance forms the root element of any large organisation's managerial initiatives. Corporate governance is about maximising organisational profits though strategic resource allocation and the management thereof (McCarthy & Puffer, 2002:631). Corporate governance is described by Nelson (2005:200) as a 'set of constraints' on both

organisational executives and shareholders. The most important of these executives is the Chief Executive Officer (CEO), who has the foremost responsibility of practising corporate governance (Nelson, 2005:197). A study done by Sohal & Fitzpatrick (2002:103) indicated that the main priorities of most CEO's are strategy oriented which includes increasing return on investment, improving customer service and improving product/service quality. Corporate governance describes what an organisation must do, how it must be done and which structures must be used to do it (Koch, 2002). This includes organisational policies, structures and management processes (Schwarz & Hirschheim, 2003:130). These processes and structures help ensure that the organisation's vision, values and strategies are realised by supporting the key decisions that are directed by corporate governance (Weill & Ross:2004). Patel (2002:3165) states that corporate governance ensures the proficient and successful use of organisational resources, thus realising their goals.

IT governance has proven to be an essential component of corporate governance (Dahlberg & Kivijarvi, 2006:194b; Carroll *et al*., 2004:233). The goal of IT governance is to manage an organisation's IT infrastructure and operations in such a fashion that it is aligned with the business strategies. In doing so, optimum business value should be delivered. For this reason, it is the responsibility of the Chief Information Officer (CIO) (Hwang, 2002:15; Koch, 2002) to ensure that IT governance is implemented in parallel with corporate governance. The CIO has the main responsibility of aligning the business with IT, developing an IT strategy, managing the IT infrastructure and supervising IT related outsourcing (Sohal & Fitzpatrick, 2002:106). The relationship between IT governance and corporate governance is so vital that Sohal & Fitzpatrick (2002: 104) strongly propagate that the CIO should not be more than one level lower than the CEO on the organisation's hierarchical executive structure. This suggestion is based on research by Sohal & Fitzpatrick (2002:98) that indicated that: Firstly, a strong relationship between CEO and CIO is critical in the assurance of the strategic use of IT in the organisation; and secondly that in organisations where the CEO's actively

participated in IT governance, the organisation was more likely to be technology focused and driven.

In addition to IT governance, risk management is also a component of corporate governance (Mena, 2002:5; Graham & Kaye, 2006:33). Hiles & Barnes (2001:25) explain that executives responsible for corporate governance are forced by stakeholders and regulatory authorities to manage an organisation's risks. For this reason risk management is an important component of corporate governance. McCarthy & Puffer (2002:631) agree and emphasise that risk management is about balancing organisational risk while corporate governance aims to maximise shareholder value. If risk management is not practiced as part of corporate governance, it might become a static exercise that puts shareholder value at risk, if not to have devastating consequences for an organisation (Beasley *et al*., 2005). The task of risk management is dedicated to the risk manager of the organisation (Graham & Kaye, 2006:4). However, this role has become so important that the position of Chief Risk Officer (CRO) (Beasley *et al*., 2005) is also implemented by many organisations. Sobel & Reding (2004:29) explain that the alignment of corporate governance and risk management is much more than just the relationship between the CEO and CRO executives: risk management is also about aligning auditors (internal and external), management and risk owners when focussing on the management of all business related risks.

Business continuity management is an essential component of risk management (Doughty, 1999; Doughty, 2002; Bakshi & Rafeq, 2005; Graham & Kaye, 2006:9). During risk management activities, the risks an organisation is exposed to are identified, assessed and prioritised. The goal of business continuity management is to, amongst others, develop response plans for each risk. These response plans should be followed in the event of a risk materialising. The business continuity manager administers all business continuity management initiatives (Lam, 2002) with the goal of ensuring that an organisation's business continuity strategy is closely integrated with the

organisation's risk management activities (Young, 2000). Often, especially in smaller organisations, the CRO also acts as the business continuity manager.

Based on the information presented the preceding sections, business continuity management relates to IT governance through risk management and ultimately corporate governance. The CEO and CRO are responsible for ensuring the healthy relationship between the CIO and business continuity manager. With the CIO traditionally focused on IT, modern responsibilities are much more business oriented. This is to the relief of the business continuity manager who are mainly business focused. Even though the relationship seems indirect, IT governance frameworks do cater for business continuity management, as discussed in the next section.

4.4 PROCESSES WITHIN IT GOVERNANCE FRAMEWORKS THAT CONTRIBUTE TOWARDS BUSINESS CONTINUITY MANAGEMENT

Various IT governance frameworks have processes dedicated to the assurance of the IT continuity in organisations. This is also true for the two IT governance frameworks referenced in this research, namely COBIT and ITIL.

The COBIT control objective that is dedicated to an organisation's business continuity is located in the Delivery & Support (DS) control area. This high-level control objective is referenced as DS4 and labelled as 'Ensure Continuous Service'. DS4 aims to ensure the uninterrupted availability of IT services in an organisation by minimising both the likelihood and impact of risks. When materialised, these risks can potentially result in the disruption of critical functions and processes.

As discussed in previous sections, the ITIL framework consists of seven sets of which Service Delivery is one example. The process element dedicated to the assurance of business continuity is discussed in the Service Delivery set and is known as IT Service Continuity Management (ITSCM). IT Service Continuity Management aims to ensure predefined levels of IT services

through the management of risks, despite the disruption of business operations.

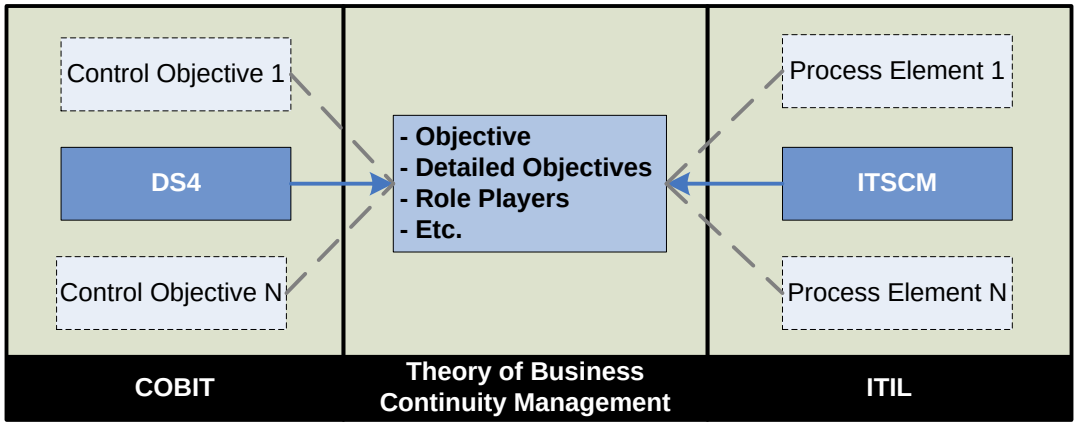

Figure 11: Using IT governance frameworks to develop a business continuity management framework

The succeeding chapter analyses the DS4 (COBIT) and ITSCM (ITIL) IT governance processes with the goal of developing a theoretical framework for business continuity management. This approach is also displayed in Figure 11.

4.5 CONCLUSION

Both IT governance and business continuity management have evolved in recent years to place more emphasis on business processes as oppose to the traditional focus on IT. IT governance is a managerial activity subservient to corporate governance. Business continuity management is a subcomponent of risk management. Similar to IT governance, risk management is also a component of corporate governance. Through risk management and corporate governance, the relationship between IT governance and business continuity management is identified. This suggestion is supported by the fact that both the COBIT and ITIL IT governance frameworks cater for business continuity management. Specifically, COBIT has a control objective referenced as DS4 – Ensure Continuous Services whereas ITIL has a process element called IT Service Continuity Management (ITSCM).

The next chapter is dedicated to the content analysis research method. The DS4 and ITSCM IT governance processes are analysed in an attempt to identify the manner in which these frameworks conceptualise business continuity management. Also, the suggested detailed objectives that could contribute towards a business continuity framework, if such objectives exist, are investigated.

CHAPTER 5
CONTENT ANALYSIS EXECUTION

5.1 INTRODUCTION

Based on the number of implementations by practitioners, the success of the COBIT and ITIL IT governance frameworks is evident. The previous chapter illustrated the relationship between business continuity management and IT governance, amongst others. The content analysis leverages the strong relationship between business continuity management and IT governance. IT governance is an established body of knowledge, spearheaded and supported by the widely acknowledged and used IT governance frameworks. What the literature of COBIT and ITIL details about business continuity management, is analysed through the use of content analysis to develop a theoretical basis for business continuity management. These aspects include the objective of business continuity management, the detailed objectives of business continuity management, the role players responsible for the continuity of an organisation and the relationship that business continuity management has with COBIT's control objectives and ITIL's process elements.

Chapter five is dedicated to the execution steps of the content analysis. The details of content analysis execution are defined in research method presented in chapter two. The content analysis was conducted by means of a software tool and the results presented in the output provided by the tool. Each of the subsequent sections presented in this chapter corresponds to the different execution steps of the framework. For each step, two tables are presented. The first table details the activities associated with each step, whereas the second table describes the results obtained from the step.

5.2 CONTENT ANALYSIS SOFTWARE TOOL PARTICULARS

A software tool was used for the content analysis to qualitatively analyse the identified text. A software package called ATLAS.ti had the required

functionality to successfully conduct the qualitative content analysis. The precise details of the software are as follows: ATLAS.ti Demo Version WIN 5.0, Build 66. More information can be retrieved from the website www.atlasti.com.

5.3 STEP 1: DEFINE RESEARCH OBJECTIVES

The content analysis presented in this chapter is one subcomponent of the research approach. The research questions, on which the content analysis is based, have been defined in chapter one. The objective of the content analysis was to identify the scope of business continuity management, specifically IT continuity from an IT governance perspective. The approach taken in this research is to analyse literature on IT governance that directly relates to business continuity management. The goal of the content analysis was to identify the objective and detailed objectives of business continuity management, the roles associated with business continuity management and how business continuity management relates to other IT governance control objectives (COBIT) or process elements (ITIL).

5.4 STEP 2: TEXT IDENTIFICATION

The second step of the content analysis aims to identify suitable text sources that might contribute towards the research objectives of the research. The unorganised text is identified using a qualitative approach and serves as a basis for the content analysis. Unorganised text includes information in different formats that has not yet been converted into organised text. Typically, unorganised text consists of literature that is likely to be relevant to the research objectives, but that needs be reformatted in the subsequent steps of the content analysis. The identification of the text sources utilised in the content analysis overlaps with the literature survey of this research. The result of the text identification step is the bundle of unorganised text.

Table 2: Steps of Content Analysis Text Identification

Step	Description
1.	Identify literature on IT governance.

Step	Description
2.	Identify literature on business continuity management.

Table 3: Results of Content Analysis Text Identification

Description
A comprehensive list of literature sources on both IT governance and business continuity management were identified. The literature was unorganised as some sources were invalid, inappropriate, uncategorised or in an inconsistent format.

5.5 STEP 3: DATA MAKING

Subsequent to the identification of the various unorganised text and before the commencement of the actual analysis, the text needs to be organised according to the resource objectives. Data making converts unorganised text into organised text by means of limited categorisation, filtering and processing. The result of the data making step is a selection of organised text.

As identified in the previous step, the scope of the content analysis is limited to IT governance frameworks. In this step, the two main IT governance frameworks namely COBIT and ITIL were identified from the literature survey and used in the content analysis. The COBIT framework used for the analysis was version four and in electronic PDF format, as published by The IT Governance Institute on the Information Systems and Control Association (ISACA) website. The ITIL framework used in this research was version two, as published by the Office of Government Commerce and is in HTML electronic format. As part of the organisation of the IT governance framework text, the COBIT components and ITIL sets are identified and appropriately grouped under each framework. A breakdown of the COBIT components and ITIL sets are presented in chapter three.

Table 4: Steps of Content Analysis Data Making

Step	Description
1.	Filter the unorganised text according to the relevance is has with the research objectives.

Table 5: Results of Content Analysis Text Identification

Description

Description
According to the research objectives, the researcher aimed to utilise existing IT governance frameworks to define business continuity management and its scope. The unorganised text was filtered so that the two most popular IT governance frameworks remain namely COBIT and ITIL.

5.6 STEP 4: TEXT ANALYSIS

Once the relevant text sources have been identified and converted into organised text, the actual analysis of the text can commence. Typically, a content analysis consists of six components, as explained in chapter two. The components need not be executed in sequential order, but must rather follow a recursive approach based on the researcher's interpretations. However, to simplify the presentation of the analysis, the execution of each component is presented in sequential order. The result of the text analysis step is a set of results that can potentially be in different formats.

5.6.1 UNITISING

The process of defining unit types is the most important step of the content analysis, as it forms the basis of the entire research.

The analysis used the same unit type for all the organised literature generated through the data making process. The unit type chosen for this research was of type 'word'. By analysing the usage of words within a given context, key concepts were identified. Once the units were identified, the contexts in which these units were used were interpreted. Based on the researcher's interpretation of these units, the conclusions of certain research objectives were derived.

The unit category chosen for this analysis was of type 'contextual units'. All units derived from the different organised literature, in this case of type 'word', were categorised under the different 'contextual unit' categories. Categories were designed according to the research objectives with the aim of grouping units to simplify the interpretation process. The following categories were identified:

- Business continuity management objective. This category identified all characteristics and attributes of business continuity management as specified by the control objective/process element. From these attributes a definition for business continuity management can be derived;

- Business continuity management detailed objectives. This category comprehensively described the detailed objectives that must be completed to ensure the achievement of the business continuity management objective;

- Business continuity management roles. This category explained the roles associated with business continuity management;

- Business continuity management input objectives. All control objectives/process elements that served as input to business continuity management were listed under this category; and

- Business continuity management output objectives. All control objectives/process elements that were dependent on the output of business continuity management were listed under this category.

Both units and categories are closely related to the quotations and coding activities during the inferring component of the content analysis. These activities are discussed in the subsequent sections. The result of the unitising component of the text analysis step was the identification of a unit type and the declaration of unit categories.

Table 6: Steps of Content Analysis Unitising

Step	Description
1.	Identify the unit type and unit category.

Table 7: Results of Content Analysis Unitising

Description

Description
The following results were achieved: • The unit type was specified as type 'word'; and • The unit categories were specified as type 'context units'. Units are assigned to categories as defined by the research objectives and according to the researcher's interpretation thereof. The following categories were identified: o Business continuity management objective; o Business continuity management detailed objectives; o Business continuity management roles; o Business continuity management input objectives; and o Business continuity management output objectives.

5.6.2 SAMPLING

After the finalisation of the unit type and unit category, the unit sampling had to be completed. As discussed in chapter two, qualitative unit sampling is conducted in a different manner compared to quantitative unit sampling.

Sample units were selected based on the defined unit categories. The sample units were selected according their relevance and possible contribution towards the research objectives, as per the researcher's interpretation thereof. The different samples extracted from the organised text remained in their original presentation. The selected samples were grouped under each IT governance framework and processed individually. The result of the sampling component of the text analysis step was the generation of different sample text.

The sampling technique used in this research followed a non-random approach and was based on the convenience sampling technique. The motivation for selecting convenience sampling was because the content analysis aimed to analyse the COBIT control objectives and ITIL process elements dedicated to business continuity management. The sample sets described the way in which IT governance conceptualises business continuity

management. The literature survey identified two sample sets. The first sample set was the DS4 control objective from COBIT and the second sample set was the ITSCM process element from ITIL. The motivation for selecting these samples sets was because each set is dedicated to business continuity management.

The objective of business continuity management was determined by investigating how the COBIT and ITIL define and explain the purpose of business continuity management. The detailed objectives of business continuity management were determined by identifying key concepts from the COBIT control objectives and the ITIL process elements.

Table 8: Steps of Content Analysis Sampling

Step	Description
1.	Using the identified unit categories, select sample sets from both the COBIT and ITIL frameworks by means of the convenience sampling.
2.	Convert the text into a format that is compatible with the software tool. Do not include figures and tables: tables should be translated during the recording process and, where appropriate, figures must be included in the analysis as separate documents.

Table 9: Results of Content Analysis Sampling

Result	Description
1.	The following sampling sets were identified using the convenience sampling technique: • COBIT: DS4 – Ensure Continuous Service; and • ITIL: IT Service Continuity Management (ITSCM).
2.	The results of the sampling activities were as follows: • COBIT DS4: One text file was created called ‘COBIT DS4.txt’; • ITIL ITSCM: One text file was created called ‘ITIL ITSCM.txt’, together with the following three images in their default format: o Fig 7.1 – Business Continuity Management Process Model, called ‘ITIL Business Continuity Management Process Model.gif’; and o Fig 7.9 – Typical management structure for business and ITSCM, called ‘ITIL Typical management structure for business and ITSCM.gif’.

5.6.3 RECORDING

Because both text sources were already in electronic text format, the recording process was fairly simple. Each text source was evaluated on an individual basis because of the uniqueness of the recording modifications. Examples of modifications include the consistent and repeatable translation of figures and tables into sentences. The translation was completed according to the researcher's discretion and interpretation. However, the different recording steps for the selected COBIT control objective and ITIL process element are detailed in Table 10 and Table 11. The result of the recording component of the text analysis step was the conversion of different units into interpretive sentences.

Table 10: Steps of Content Analysis COBIT Recording

Step	Description
1.	Locate the High Level Control Objective section of the particular control objective. Covert the Information Criteria figure into sentences using the following format: The [Primary]/[Secondary] objective(s) of [Control Objective] is/are [Information Criteria N], [Information Criteria N + 1].
2.	Locate the High Level Control Objective section of the particular control objective. Convert the IT Governance Focus Area figure into sentences using the following format: The [Primary]/[Secondary] IT governance focus area(s) of [Control Objective] is/are [Information Criteria N], [Information Criteria N + 1].
3.	Locate the High Level Control Objective section of the particular control objective. Convert the IT Resource figure into sentences using the following format: [Control Objective] focuses on the following organisational resources: [IT Resource N], [IT Resource N + 1].
4.	Locate the Management Guidelines section of the particular control objective. Convert the Input table and Output table into sentences using the following format: [From Column] – [Control Objective Name] serves as [input]/[output] to [Control Objective] by means of [Inputs Column].
5.	Locate the Management Guidelines section of the particular control objective. Convert the activities section of the RACI Chart into sentences (ignore the role players) using the following format: The activities which [Control Objective] is accountable for are [Activity Column N], [Activity Column N + 1]…

Step	Description
6.	Locate the Management Guidelines section of the particular control objective. Convert the functions section of the RACI Chart into sentences (ignore the activities) using the following format: The role players for [Control Objective] are [Role Player N],[Role Player N + 1]…
7.	Locate the Management Guidelines section of the particular control objective. Convert the Activity Goals figure under the Goals and Metrics section into sentences using the following format: The activity goals of [Control Objective] are [Activity Goal N], [Activity Goal N + 1]…
8.	Locate the Management Guidelines section of the particular control objective. Convert the Key Performance Indicators figure under the Goals and Metrics section into sentences using the following format: The key performance indicators of [Control Objective] are [Key Performance Indicator N], [Key Performance Indicator N + 1]…
9.	Locate the Management Guidelines section of the particular control objective. Convert the Process Goals figure under the Goals and Metrics section into sentences using the following format: The process goals of [Control Objective] are [Process Goal N], [Process Goal N + 1]…
10.	Locate the Management Guidelines section of the particular control objective. Convert the Process Key Goal Indicator figure under the Goals and Metrics section into sentences using the following format: The process key goal indicators of [Control Objective] are [Process Key Goal Indicator N], [Process Key Goal Indicator N + 1]…
11.	Locate the Management Guidelines section of the particular control objective. Convert the IT Goals figure under the Goals and Metrics section into sentences using the following format: The IT Goals of [Control Objective] are [IT Goal N], [IT Goal N + 1]…
12.	Locate the Management Guidelines section of the particular control objective. Convert the IT Key Goal Indicator figure under the Goals and Metrics section into sentences using the following format: The IT Key Goal Indicators of [Control Objective] are [IT Key Goal Indicator N], [IT Key Goal Indicator N + 1]…

Table 11: Steps of Content Analysis ITIL Recording

Step	Description

Step	Description
1.	Locate the typical responsibilities for ITSCM during normal operation figure (Fig 7.10). Convert the figure into sentences using the following format: During normal operations, [Role] has/have the ITSCM responsibilities of [Responsibility N], [Responsibility N + 1]…
2.	Locate the typical responsibilities for ITSCM during times of crisis figure (Fig 7.11). Convert the figure into sentences using the following format: During times of crises, [Role] has/have the ITSCM responsibilities of [Responsibility N], [Responsibility N + 1]…

Table 12: Results of Content Analysis COBIT DS4 Recording

Result	Description
1.	One sentence of type primary was created consisting of two objectives. One sentence of type secondary was created consisting of one objective.
2.	One sentence of type primary was created consisting of two IT governance areas. One sentence of type secondary was created consisting of three IT governance areas.
3.	One sentence was created consisting of four organisational resources.
4.	Five input and eight output sentences were created.
5.	One sentence was created consisting of eleven activity entries.
6.	One sentence was created consisting of eleven role players.
7.	One sentence was created consisting of three activity goals.
8.	One sentence was created consisting of four key performance indicators.
9.	One sentence was created consisting of three process goals.
10.	One sentence was created consisting of four process key goals Indicators.
11.	One sentence was created consisting of three IT goals.
12.	One sentence was created consisting of one IT key goal indicator.

Table 13: Results of Content Analysis ITIL Recording

Result	Description
1.	Four sentences were created, one for each role, with a total of 16 responsibilities.
2.	Four sentences were created, one for each role, with a total of 13 responsibilities.

5.6.4 SIMPLIFYING

The researcher performed various text simplifying activities on the text sources after the completion of the recording activities. The aim of these activities was to improve the quality of the text to simply the interpretation. The text simplification process of this research was fairly elementary: the researcher only conducted text cleaning and specific packaging activities. As mentioned previously, a recursive process of analysing the text were followed, even more so during the simplification process. The simplifying component completed final modifications on the sample text so that it was completely compatible with the software tool.

Table 14: Steps of Content Analysis Simplifying

Step	Description
1.	Remove all illegal characters (as specified by the software tool) by either replacing them with a word, or by excluding them from the text.
2.	Covert the images to a format that is compatible with the software tool.

Table 15: Results of Content Analysis Simplifying

Result	Description
1.	The following characters were removed: • COBIT DS4: Three occurrences of '%' were replaced with 'percentage'. Two occurrences of '#' were replaced with 'number'; and • ITIL ITSCM: All JavaScript and hyperlink units were converted into normal text units during the sampling process.
2.	The following images were converted: • 'ITIL Business Continuity Management Process Model.gif' was converted to 'ITIL Business Continuity Management Process Model.jpg'; • 'ITIL Risk Assessment Model.gif' was converted to 'ITIL Risk Assessment Model.jpg'; and • 'ITIL Typical management structure for business and ITSCM.gif' was converted to 'ITIL Typical management structure for business and ITSCM.jpg'.

5.6.5 INFERRING

Inferring is the actual analysis process that gets executed on the organised text. During the inferring process, a software tool was used to perform the interactive hermeneutic activity of identifying quotations and assigning it to

appropriate codes. In addition to this, the tool also partitioned the text into the desirable units and represented the results of the analysis in a visual format as to simplify interpretation of the results. The 'code and unit analysis' inferring technique was used, which allowed for the qualitative interpretation of organised text. The result of the inferring component of the text analysis step was the completion of the analysis. The results obtained from the inferring component were later converted in a visual presentation.

Table 16: Steps of Content Analysis Inferring

Step	Description
1.	Create a new hermeneutic unit using the ATLAS.ti software tool.
2.	Import all the sample sets created as P-Docs. The terminology 'P-Docs' refers to the text sources used by the tool.
3.	Create codes according to the unit categories defined during the unitising and categorising content analysis component. Create an additional parent code to which all the other codes are linked.
4.	Create one network view for each of the codes linking to the parent code. These network views are used for the visual interpretation of the content analysis.
5.	Identify key units from the different P-Docs that contribute towards the codes created. Create quotes from these units and link each quote to the appropriate code.
6.	Import the different codes together with the quotes assigned to it, in the appropriate network view.

Table 17: Results of Content Analysis COBIT Simplifying

Result	Description
1.	One empty hermeneutic unit was created.
2.	The following documents were imported as P-Docs: • COBIT DS4.txt; • ITIL ITSCM.txt; • ITIL Business Continuity Management Process Model.jpg; and • ITIL Typical management structure for business and ITSCM.jpg.

Result	Description
3.	Six codes were created. Five codes were based on the unit categories defined and one code as the parent code to which the other five codes are link. The codes were named as follows: • Business Continuity Management (BCM) – this is the parent code; • BCM Objective; • BCM Detailed Objectives; • BCM Roles; • BCM Inputs; and • BCM Outputs.
4.	Four network views were created. One network view was created for the input and output codes as to simplify the utilisation of shared quotes. The following network views were created: • BCM Objective network view; • BCM Detailed Objective network view; • BCM Roles network view; and • BCM Inputs & Outputs network view.
5.	During the interpretation of each of the P-Docs, the following amount of quotes were assigned to each code: • 20 quotes were assigned to the BCM Objective code; • 105 quotes were assigned to the BCM Detailed Objectives code; • 18 quotes were assigned to the BCM Roles code; • 10 quotes were assigned to the BCM Input code; and • 12 quotes were assigned to the BCM Output code.

Result	Description
6.	The following codes with the relevant quotes assigned to it, were assigned to network views: • The BCM Objective code was assigned to the BCM Objective network view; • The BCM Detailed Objectives code was assigned to the BCM Detailed Objectives network view; • The BCM Roles code was assigned to the BCM Roles network view; and • The BCM Input code and BCM Output code were assigned to the BCM Inputs & Outputs network view.

5.6.6 NARRATING

The narrating component of the content analysis reports on the results obtained from the inferring component. Typically, the result of the inferring component is unique to the software tool used. In this particular research, the software tool made use of network views. The quotes derived from units were assigned to codes that were similar to the unit categories defined. The end result of the exercise was a hierarchical tree(s) of key words that had to be interpreted. Table 18 details the different reports generated from the software tool as per research objective:

Table 18: Research Objectives and Related Content Analysis Reports

Research Objective	Report
Business continuity management objective	Figure 12: Business Continuity Management Objective
Business continuity management detailed objective	Figure 13: Business Continuity Management Detailed Objectives
Business continuity management roles	Figure 14: Business Continuity Management Roles
Business continuity management and related control objectives/process elements.	Figure 15: Business Continuity Management Inputs & Outputs

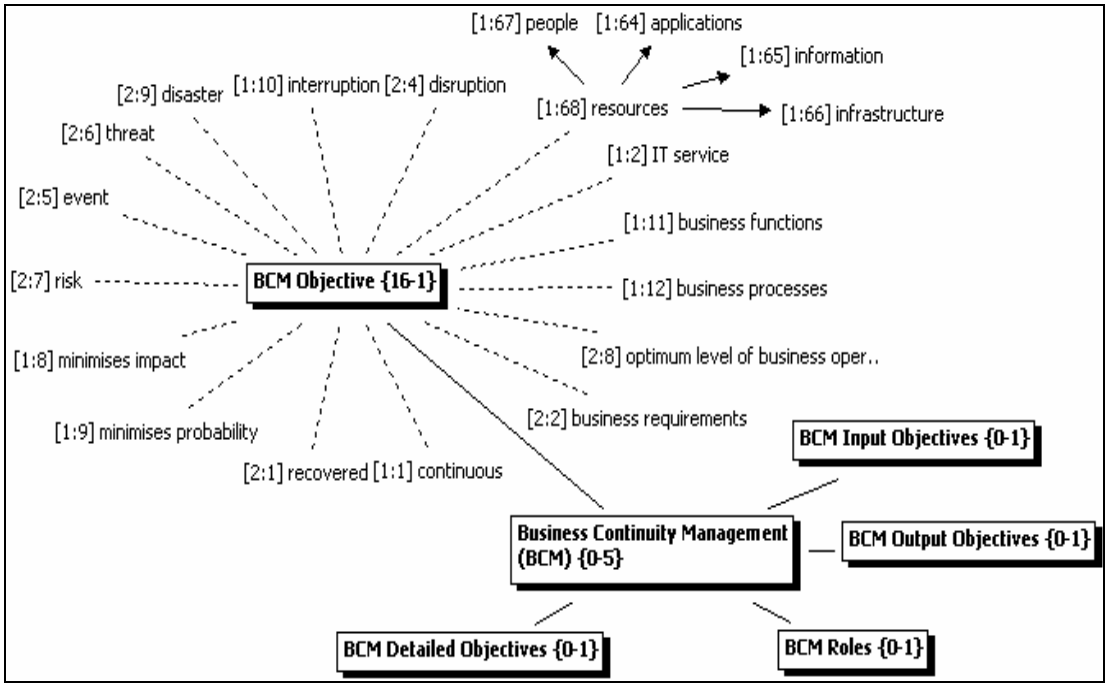

Figure 12: Business Continuity Management Objective

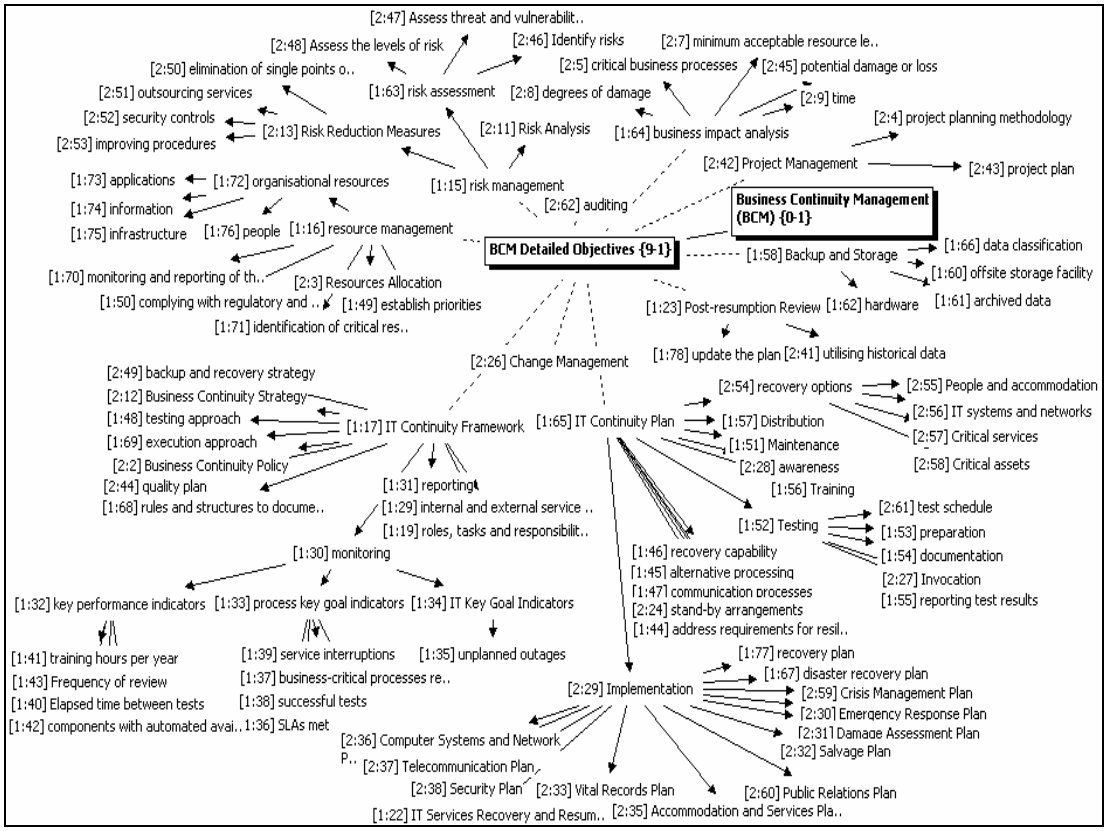

Figure 13: Business Continuity Management Detailed Objectives

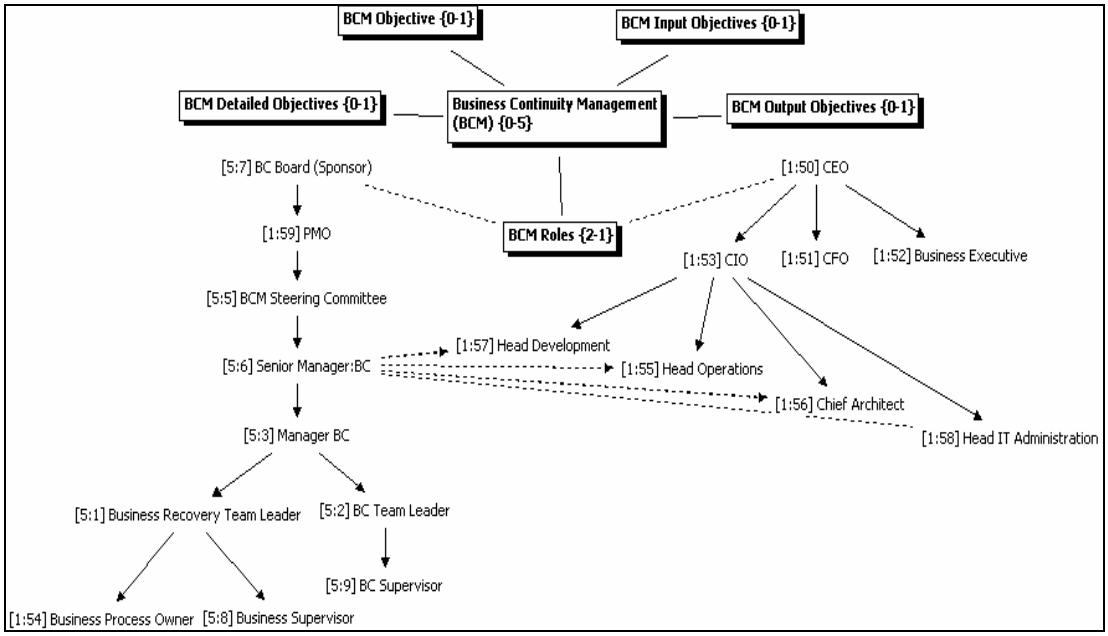

Figure 14: Business Continuity Management Roles

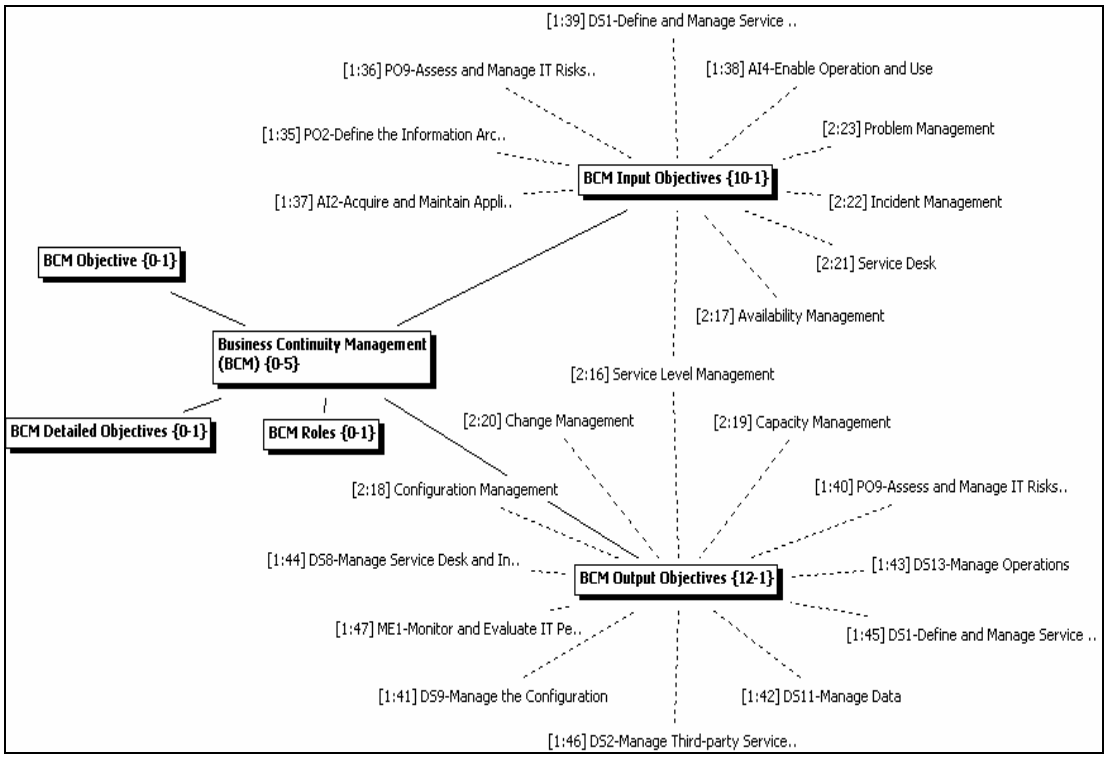

Figure 15: Business Continuity Management Inputs & Outputs

5.7 STEP 5: INTERPRETATION AND CONCLUSIONS

Once the execution of the different content analysis components is complete, the results can be interpreted and the necessary conclusions can be formulated. Using the reports generated from the content analysis' narrating

component, the quotations supporting the different research objectives was interpreted. The results of the interpretation and conclusions of the content analysis are presented in the subsequent chapter.

5.8 STEP 6: VALIDATION OF CONCLUSION

To validate the results of the content analysis, the derived interpretations and conclusions must be both reliable and valid.

As a result of the qualitative nature of the content analysis, no additional resources were needed nor permitted during the execution of the analysis. For this reason, the reliability of the analysis is limited to the step-by-step documentation of the execution process. Throughout the analysis, various tables documented the execution steps as well as the actual results of each step.

The validation of the content analysis made use of content, empirical and social validity tests and was limited to the interpretation of the different units of the organised text. The content validity test was automatically successful: the quotations identified to support the different research objectives used existing units derived from organised text. Similarly, as the analysis was based on the utilisation of existing organised literature, the empirical validation was also supported by the analysis. The social validity of the test was more complex than the content and empirical tests. The conclusions derived from the analysis were presented to the participants of the empirical study. The success of the social validation step was based on whether the candidates accepted the results of the interpretations of the content analysis (presented in the next chapter). Table 19 details the results of the social validation test:

Table 19: Research Objectives and Related Content Analysis Reports

Research Objective	Organisation			
	A	B	C	D
Business continuity management objective	Yes	Yes	Yes	Yes
Business continuity management detailed objective	Yes	Yes	Yes	Yes

Research Objective	Organisation			
	A	B	C	D
Business continuity management roles	Yes	Yes	Yes	Yes
Business continuity management and related control objectives/process elements.	Yes	Yes	Yes	Yes

Each research objective was presented in a document format to the participants of the empirical study. The validation was done after the completion of the interviews as not to influence their contributions to the research. In the case where multiple participants were interviewed, they had to unify their answers to create one response per organisation. The result of the social validation clearly indicated that all participating organisations agreed that the content analysis' interpretations are applicable to the relevant research objectives.

5.9 CONCLUSION

The research method consists of a content analysis on selected parts of the COBIT and ITIL IT governance frameworks. The objective of the content analysis was to present the objective, detailed objectives, the roles required to ensure the continuity of an organisation and lastly, the relationship that business continuity management has with COBIT and ITIL.

The result of the content analysis was obtained with the assistance of a software tool. The content analysis execution was presented as a list of sequential steps (as defined and explained in chapter two) that detailed both the predefined steps and the results obtained. The result of the content analysis was successfully validated through various methods. The next chapter is dedicated to the interpretation of these results.

CHAPTER 6
CONTENT ANALYSIS INTERPRETATION

6.1 INTRODUCTION

The previous chapter presented the execution of the content analysis on the COBIT and ITIL IT governance frameworks. The goal was to analyse the control objectives (COBIT) and process elements (ITIL) of each framework that are dedicated to business continuity management. In this chapter, the results achieved from the content analysis are interpreted. The content analysis focused on four main categories. The first category defined and identified the objectives of business continuity management. The second category was dedicated to the detailed objectives of business continuity management. The relationship between the objectives and detailed objectives of business continuity management was presented in chapter one. The third category was aimed at identifying the typical role players that could contribute towards the success of business continuity management. Lastly the input and output categories identified how business continuity management relates to other COBIT control objectives and ITIL process elements.

In this chapter the various keywords derived from the content analysis are interpreted. Where possible, the interpretations are complemented with additional literature sources.

In chapter six, the following secondary research questions are answered:

- What is the objective of business continuity management?
- What are the detailed objectives of business continuity management?
- Who are the typical role players responsible for business continuity management?

- How should business continuity management be integrated with the different IT governance frameworks?

6.2 BUSINESS CONTINUITY MANAGEMENT OBJECTIVE

The objective of business continuity management is based on the results of the content analysis, as indicated in Figure 12. The results of the content analysis' business continuity management objective can be grouped into two parts. The first part focuses on the environmental factors influencing the continuity of an organisation, whereas the second part deals with the attributes of business continuity management. The definition and objective of business continuity management are determined by these attributes.

6.2.1 ENVIRONMENTAL FACTORS INFLUENCING BUSINESS CONTINUITY MANAGEMENT

The content analysis identified three types of environmental factors that influence business continuity management namely risks, threats or events. Each of these types is now discussed with reference to supporting literature sources.

6.2.1.1 RISK

Jones (2005:44) states that risk is the best described as the uncertainties an organisation has during the conduction of daily business activities. Risk is based on the decisions made by an organisation and the resulting uncertainties the decision creates. Most decisions are typically influenced by both positive and negative factors that are also referred to by Graham & Kaye (2006:91) as opportunities and threats respectively. The identification and comparison between the positive and negative factors result in the decision maker making an informed choice. Should the positive factors outweigh the negative factors, the decision maker will usually choose to proceed with decision despite the presence of the negative factors. The decision consequently introduces risks based on the negative factors taken into

consideration during the decision making process. Therefore, a risk is defined as follows:

A risk is a calculated uncertainty based on the probability of the materialisation of a negative factor that contributed to an informed decision that was made.

From this definition three important conclusions can be derived that distinguish a risk from a threat or event: Firstly, a risk can never be unforeseen and the materialisation of the risk is always based on probabilities. As a result of a risk being derived from the cognitive process of decision making, the negative factors contributing to an informed decision are predefined. Secondly, a risk can be eliminated. By reversing the decision, the negative factors cannot materialise and consequently the risk is removed. The probability of the risk materialising is can also be decreased by allocating specific resources to minimise the likelihood of the risk materialising. Thirdly, the materialisation of a risk will have anything from a low to critical negative impact on an organisation. As a risk is based on a negative factor, the materialisation of a risk will also have a harmful impact on an organisation. However, what differentiates a risk from a threat and event is the fact that the level of impact it has on the organisation is not taken into account.

Lastly, Hiles & Barnes (2001:31) categorise risks under the following categories:

- Strategic risks e.g. inaccurate market segmentation, poor marketing plan and wrong acquisitions;

- Financial risks focus on financial controls like fraud, treasury risks, credit control, etc.;

- Operational risks is usually a result of human interaction, e.g. design blunders, inaccurate calculations or decisions;

- Commercial risks typically focus on business interruptions. Examples include supplier failure, inadequate compliance or even the loss of a an executive; and

- Technical risks are mostly associated with physical assets such as equipment failure, infrastructure disruption, IT downtime, fires, explosions, etc.

By categorising risks into any of these categories, organisations might be able to manage these risks more effectively and efficiently.

6.2.1.2 THREAT

Unlike a risk, a threat is not based on a decision making process. A threat, like an event, can be a random factor (internal or external to the organisation) that influences the organisation negatively. A threat can be either foreseen or unforeseen. A threat consists of all factors that will have a negative impact on the organisation should it materialise. What distinguishes a threat from an event is the fact that a threat will definitely impact an organisation negatively. A threat is also more likely to be recognised prior to its materialisation as it typically has a much more devastating effect on an organisation when compared to an event. The concept of a threat is defined as follows:

A threat is any foreseen or unforeseen environmental factor that has a severe negative impact on the continuity of an organisation, should it materialise.

6.2.1.3 EVENT

An event is very similar to a threat with the exception that should it materialise, it might not have a negative impact on the organisation. Typically, events are factors that have a low or moderate impact on the organisation. As a result, events are often not recognised by the organisation prior to its materialisation. Like a threat, an event also caters for both internal and external environmental factors. An event is defined as follows:

An event is any foreseen or unforeseen malicious environmental factor that could have a limited negative impact on the continuity of an organisation, should it materialise.

Needless to say, events occur more frequently than threats. The majority of these events are recurring, which means that if an organisation follows a proactive approach, these events can be resolved with minimal disruption and effort – if not completely prevented.

6.2.2 DEFINING THE OBJECTIVE OF BUSINESS CONTINUITY MANAGEMENT

The result of the content analysis identified various characteristics of business continuity management. Business continuity management aims to minimise both the probability and impact of risks, threats and events that can disrupt the optimum level of business operations required. Should the continuity of an organisation be interrupted, business continuity management aims to recover the business operations by restoring the necessary business processes, functions and services. Naturally, business continuity management focuses on all resource areas in the organisation.

The result of the content analysis, as discussed in the previous section, is supported by different literature sources. Business continuity management is about establishing both preventive and responsive plans (Herbane *et al*.., 2004:435) to avoid or limit the impact that a disruption might have on an organisation. Manning (1999:243) motivates that business continuity management aims to prevent the discontinuation of organisational activities as a result of the failure of critical processes. Business continuity management is about the evaluation of risks, threats or events and the management thereof, to restore the organisation's environment to its original state prior to the disruption. Hiles & Barnes (2001:22) explains that business continuity management is about being prepared to restore critical business operations to a state that can provide the required level of services to customers while limiting the financial impact caused by the disruption.

Calderon (2003:20) states the implementation of a business continuity management plan should ensure the continuous operations of an organisation so that the strategic objectives can be met. Business continuity management focuses on the potential disruptions that an organisation is exposed to, ranging from a low to critical impact. As highlighted in the content analysis, the success of an organisation is no longer primarily dependent on the IT infrastructure alone – after all, IT processes were originally designed to support, simply and improve business operations. However, the IT activities in an organisation are still of vital importance to ensure an organisation's business continuity. Sayana (2005) believes that an organisation's business continuity management should still mainly focus on IT. Yet, even more critical than IT is the integration between IT and the business processes of an organisation (Sayana, 2005; Price, 2004:34). Today, the major focus of business continuity management is on the critical business processes in an organisation (Doughty, 2002). Graham & Kaye (2006:10) define this as a holistic managerial activity. The goal of business continuity management has rightfully been restored to focus on, what Cummings (2005:s4) refers to as the 'business' in business continuity management.

The objective of business continuity management is defined as follows:

Business continuity management is the analysis of risks, threats and events, the impact it might have on an organisation and the design of preventive and response plans, with the objective of sustaining the continuity of an organisation.

6.3 THE DETAILED OBJECTIVES OF BUSINESS CONTINUITY MANAGEMENT

A comprehensive list of detailed objectives of business continuity management was identified during the content analysis. These detailed objectives include resource management, risk management, guidelines for business continuity management, the development of a business continuity management plan, post resumption review, project management, change

management and auditing. A summary of these detailed objectives and their content is presented in Figure 13. In the subsequent sections, the details of each of these detailed objectives, together with supporting literature sources, are presented.

6.3.1 RESOURCE MANAGEMENT

As mentioned previously, resource management forms the basis of business continuity management. Based an organisation's resources, different services are used to enable the daily operations of organisations. The different aspects of resource management that relate to business continuity management are presented in Figure 16, as interpreted through the content analysis.

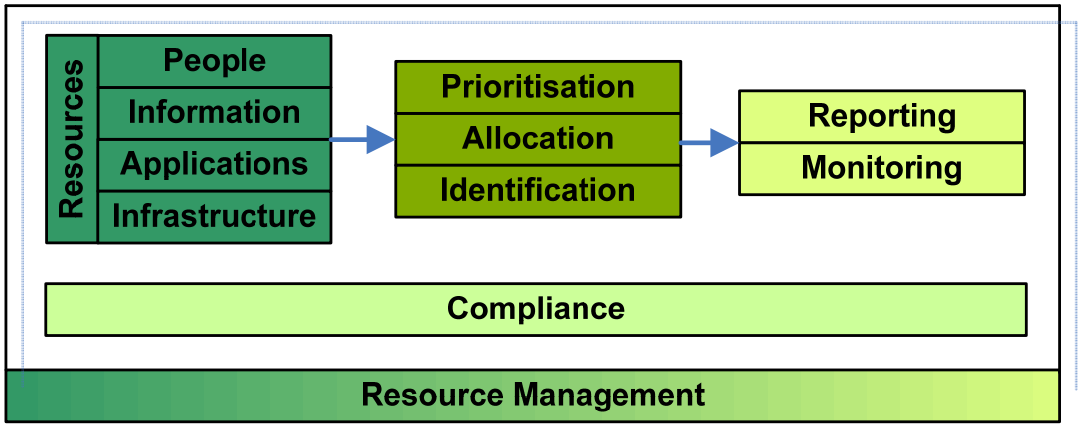

Figure 16: Business Continuity Management Detailed Objective - Resource Management

The core resources of any organisation are infrastructure, applications, information and people. Infrastructure resources are typically tangible and include buildings, equipment, hardware, etc. Once an organisation's infrastructure is in place, applications can be deployed. Applications are also known as software and act as a facilitator of business processes. If implemented and used successfully, information can be derived from applications and is often used to simplify decision making. People must interpret information, which is the last type of resource. People are all individuals that participate in the daily business operations, which eventually contribute to the success of a business.

The first step in resource management is to identify all resources critical to the continuity of an organisation, regardless of its contribution. During this process, additional resources can also be identified to improve business continuity. Once finalised, the different resources must be categorised according to the resource type and then prioritised according to the contribution it has to the success of an organisation. The monitoring of each of these resources, despite its priority, is essential. Even though all resources will be monitored, the reporting of critical resources is more valuable than that of less critical resources. Finally, organisations must ensure that all resources and the activities related to it must be compliant with regulatory and contractual requirements. Some of these external requirements include the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act and the Sarbanes-Oxley Act (Price 2004:34).

Even though Doughty (2002) believes that the management of resources must be categorised under risk management (as oppose to being on its own), he still acknowledges the importance of resource management to ensure business continuity. The content analysis also failed to identify finance as one of the core organisational resources.

6.3.2 RISK MANAGEMENT

Once the organisational resources have been identified and prioritised through resource management, the risks associated with each of the resources should be managed. Risk management is about eliminating or minimising the risks that threaten the continuity of an organisation (Beasley *et al*., 2005) or to reduce the environmental uncertainties that exists in the organisation (Jones, 2005:44). Graham & Kaye (2006:92) explain that risk management – specifically the assessment of risk and the business impact analysis – are not optional to ensure the resilience of an organisation. The content analysis identified that the risk management detailed objective consists of three main steps that are dependant on each other and that should be executed in sequential order, as indicated in Figure 17.

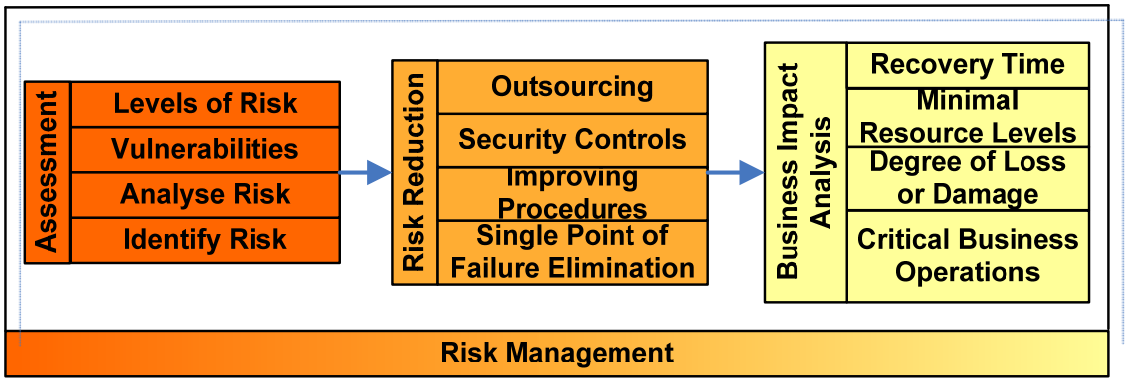

Figure 17: Business Continuity Management Detailed Objective - Risk Management

The first step of risk management (focussing on business continuity) is the assessment of the different risks to which an organisation is exposed. After the identification and analysis of each risk, the vulnerabilities that the organisation has to these risks should be identified. The final activity of the risk assessment is to categorise the risk and vulnerability to an appropriate risk level, as discussed in factor analysis quadrant (Figure 29).

After the risk assessment, an organisation should attempt to reduce the likelihood of the risk materialising and impact when the risk does materialise (Jones, 2005:44; Hiles & Barnes, 2001:88). The best way to reduce a risk is to completely eliminate it – specifically where single-point-of-failures are present. In cases where risks cannot be completely eliminated, the focus should be shifted to the improvement of procedures and security controls in an attempt to minimise the impact of the risk. If risk elimination or minimisation not be feasible or cost effective, an organisation should consider making use of outsourcing as an alternative way to manage risks (Graham & Kaye, 2006:129). During the risk assessment, the organisation should identify the likelihood of the risk materialising and decide whether the organisation is willing to accept the level of risk (Lam, 2000:20).

The final step of risk management is the business impact analysis activity. Whereas the previous two steps (risk assessment and risks reduction) focuses on the risks associated with the organisational resources, business impact analysis is about analysing the impact that the materialisation of the

risk can have on critical business operations Sayana (2005). Hiles & Barnes (2001:35,139) explain that the business impact analysis forms a critical basis for future business continuity management activities. It not only assesses the impact of the risks in the organisation but also identifies information that can be used in business cases to obtain executive commitment for a business continuity management implementation. The business impact analysis should identify the maximum tolerable outage (MTO), resumption time objective (ETO), recovery time objective (RTO) and the recovery data objective (RDO). The MTO is the maximum time period in which the recovery operations must be completed before an organisation is prevented from achieving its objectives. The ETO stipulates how fast the organisation should be able to continue with the business operations even though the organisation might not have fully recovered (Lam, 2000:21). Calderon (2003:20) explains that the RTO is to determine how soon the different organisational resources should be recovered. Closely related, is the RDO that details the age of the data to be recovered (Sayana, 2005). Once the identification of critical business operations and the associated resources have been completed, the different levels of loss for each operation must be determined. These losses can only materialise as a result of the failure of specific resources that was identified in the resource reduction activity. The next activity is to specify the minimum level of resources needed to continue with daily operations. Lastly, the minimum recovery time in which all resources should be restored to support the minimum level of business operations, must be determined.

Even though Manning (1999:244) differentiates between the business impact analysis and the assessment and reduction of risks, he agrees that both form an important part of the continuity of an organisation. Doughty (2002) explains that even though business continuity management is a subcomponent of risk management, certain risk management activities (like those presented in Figure 17) form the basis of business continuity management.

6.3.3 BUSINESS CONTINUITY MANAGEMENT GUIDELINES

Once the management of the risks associated with the different organisational resources have been established, the guidelines for business continuity management can be developed. Upon completion, a business continuity management plan can be formulated. The different steps that make up the business continuity management guidelines (as interpreted through the content analysis) are listed in Figure 18:

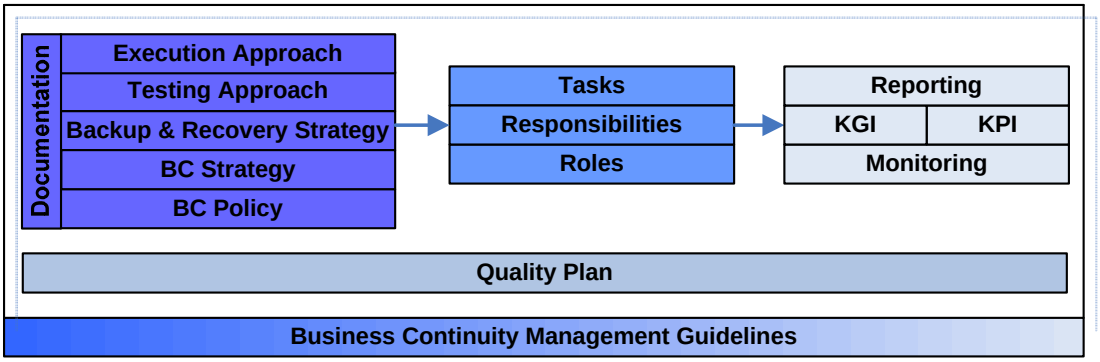

Figure 18: Business Continuity Management Detailed Objective - Guidelines

The first step of the business continuity management guidelines focuses on a set of documents. These documents include the organisation's policies, strategies and approaches to the management of business continuity. The two most important documents are the business continuity management policy and strategy. A business continuity management policy forms the basis of all business continuity management initiatives in the organisation (Doughty, 2002). The business continuity management policy specifies the position taken by organisation to ensure business continuity and includes the definition, purpose, scope, approach and managerial commitment of the business continuity management implementation (Graham & Kaye, 2006:78 – 83). Doughty (1999) mentions that a business continuity management strategy is closely aligned with the results of the business impact analysis in the risks management detailed objective. Hiles & Barnes (2001:27) also includes the business continuity strategy as is one component of a business continuity management framework. The strategy states the main objective of all business continuity management implementations and services as a guideline for the business continuity management plan. Manning (1999:244) agrees that business continuity management strategy is the fundamental basis for all business continuity management activities. The backup and recovery strategy formulates the main objectives and guidelines for the

backup and recovery of data, files and documents, amongst others. The testing and execution approach describe and motivate the steps taken during the testing and execution of the business continuity management plan.

The next step focuses on the roles, responsibilities and tasks of selected personnel in the organisation who will be involved in business continuity management. Lam (2000:21) suggests that existing roles should service as a basis and that individuals should be grouped with experienced leaders. The first activity is to identify the different roles needed to ensure effective business continuity management. The roles related to business continuity management are discussed later in this chapter. Based on each role, the different responsibilities that characterise the role must be recognised. The success of each task is dependant on how well the subsequent tasks of the responsibility are completed.

Key areas within the organisation should be monitored to ensure the success of the responsibilities and tasks execution. Once the monitoring environment and techniques have been finalised, specific key goal indicators (KGI) and key performance indicators (KPI) must be specified (Hiles & Barnes, 2001:34). These indicators should continuously measure and assess the performance of the business continuity plan. A KGI is the low level monitoring of an organisation's performance compared to specific targets. A KPI is the high level measurement of an organisation's overall performance in a specific area. Usually, different KGI's contribute to a single KPI. The reporting of an organisation's performance against the declared KGI's and KPI's is essential to the success and improvement of a business continuity management plan.

Lastly, it is important to note that the business continuity management guidelines should follow a quality plan to ensure the excellence of all activities.

6.3.4 BUSINESS CONTINUITY MANAGEMENT PLAN

Based on the business continuity management guidelines, a business continuity management plan should be develop to document the responsive steps to be executed when a disruption materialises (Manning, 1999:244). In addition to the responsive steps, a business continuity management plan also describes the preventive measures an organisation should implement to avoid potential disruptions from occurring (Hiles & Barnes, 2001:25). Calderon (2003:20) explains that a business continuity management plan implements processes, knowledge and technology to ensure the continuity of an organisation's information systems. A business continuity management plan consists of various other continuity plans focussing on specific areas in the organisation. The detailed steps of a business continuity management plan, as identified through the content analysis, are presented in Figure 19.

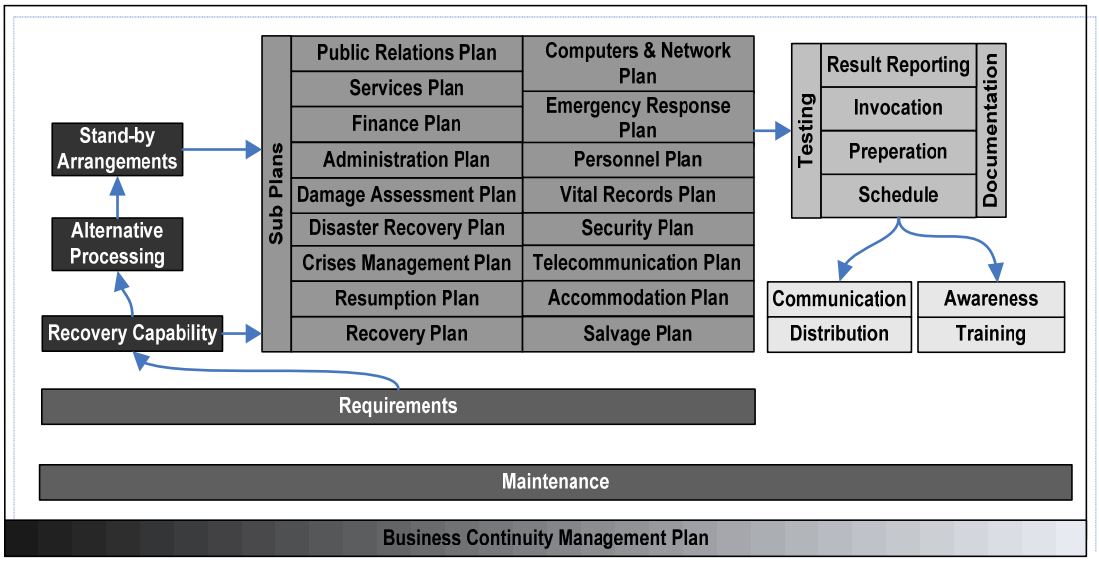

Figure 19: Business Continuity Management Detailed Objective - Plan

At the core of any business continuity management plan is the organisation's continuity requirements. These requirements relate back to the critical business operations activity in the business impact analysis step of the risk management detailed objective. The critical business operations describe the core actions performed by the organisation to ensure its continuity. The requirements activity focuses on what is needed by the organisation to perform these core actions.

Based on the requirements, the recovery capability of the organisation should be documented. The recovery capability details the different ways in which an

organisation can recover from a disruption and to what degree the recovery can be completed. The recovery capability serves as input to the sub business continuity management plans and also the alternative processing and stand-by arrangements steps.

The alternative processing step presents different processing options for critical business processes. These options should be utilised when the normal processing capabilities are disrupted. It might be that the continuity of the organisation is in danger because of the disruption of the normal processing method. However, by temporarily implementing alternative processing methods, the organisation's operations can continue.

Stand-by arrangements are the alternative processing arrangements with both external parties and different departments in the organisation. These arrangements are typically written documents detailing the agreements and scenarios when the agreement becomes active. These stand-by arrangements should become active when disruption materialises.

The business continuity plan, together with the sub continuity plans discussed in the following section, should focus on preventive and responsive controls (Sayana, 2005). Many of these plans should also include what Hiles & Barnes (2001:57) call 'Multilateral Continuity Planning', which extends business continuity management planning to also include the organisation's dependencies on partners, suppliers and customers. The following points briefly describe the different plans:

- Recovery plan: The recovery plan focuses on the restoration of business operations that have been disrupted;

- Disaster recovery plan: Documents the process of restoring the business continuity disruptions caused by risks, threats and events. Typically, disaster recovery plans are more focused on technology (Doughty, 2002; Hiles & Barnes, 2001:26; Herbane *et al*., 2004:435);

- Crisis management plan: Details the managerial activities required when a crisis occurs in the organisation. A crisis is defined as an organisation's sudden response a disruption (Hiles & Barnes, 2001:47). Doughty (2002) argues that the main goal of this plan is to minimise the impact of a crisis, whereas Hiles & Barnes (2001:44) argue that crisis management is also about implementing preventive measures to avoid a crisis from materialising. Graham & Kaye (2006:351) state that the plan should focus on the wider impact which the disruption has on the organisation and not only on the disruption itself;

- Resumption plan: The resumption plan describes the process of migrating from any temporarily recovery implementations back to the original state prior to the recovery process (Sayana, 2005);

- Emergency response plan: Details the organisation's immediate response to a disruption with the aim of minimising the impact it has on the organisation (Hiles & Barnes, 2001:178). This plan is developed to ensure consistent and accurate decisions to be taken at the time of the disruption;

- Damage assessment plan: Describes how the organisation should go about assessing the damage after a disruption. Typically, this plan is formulated and executed by specialist representing different departments in the organisation and who can accurately calculate the damage and consequences caused by the disruption (Hiles & Barnes, 2001:118);

- Administration plan: This plan documents the different administration tasks to support the recovery process of a disruption (Hiles & Barnes, 2001:117). One such example is the establishment of a emergency control centre/command centre;

- Finance plan (Hiles & Barnes, 2001:212): Details the financial prioritisation, allocation and utilisation to cover the expenditures during a recovery process;

- Services plan: Focuses specifically on the recovery of all the services obtained from third parties and also the services presented to third parties by the organisation;

- Public relations plan: The activities planned to manage the public's conceptualisation and responses during the time of a disruption. This includes all interaction with the media (Hiles & Barnes, 2001:212), shareholders and competitors;

- Salvage plan: Typically, a salvage plan documents the agreements with third party vendors to deliver specialised services to assess, stop and stabilise the impact of a business interruption. These services are aimed at preventing the business disruption from escalating and therefore attempting to minimise the recovery efforts as much as possible (Hiles & Barnes, 2001:161);

- Accommodation plan: This plan details the temporarily accommodation of staff and working premises (Hiles & Barnes, 2001:211) should the location of the organisation be unavailable;

- Telecommunications plan: The telecommunications plan describes the restoration of the organisation's telecommunications infrastructure. Hiles & Barnes (2001:161) emphasise that a typical modern organisation's telecommunications continuity plan should be closely aligned with their disaster recovery plan as telecommunications has become mostly technology driven;

- Security plan: Documents the security initiatives of the organisation during the recovery of a disruption which includes not only physical security measures but also IT related security;

- Vital records plan: The vital records plan details the recovery procedures planned to restore the vital data needed by the organisation. Typically, the continuity assurance of electronic data should be detailed in the disaster recovery plan. Hiles & Barnes (2001:160) adds that the vital records plan should also ensure that hard copies of data do not get lost in the case of a disaster;

- Personnel plan: Describes the organisation's plan to manage personnel during the time of a recovery. Some of the elements detailed in a personnel plan include, amongst others, the handling of physical injuries, treatments, trauma psychology, organisational politics, hostage and kidnapping scenarios and any communications with relatives (Hiles & Barnes, 2001:279 – 288); and

- Computers and network plan: This plan is about restoring the organisation's IT infrastructure which includes computers and networks (Sayana, 2005). Even though the content analysis has categorised this plan separately, it should form part of the disaster recovery plan, which mainly focuses on information technology.

Once the different plans have been completed, each plan should be tested. During the testing of the plans, each activity should be documented (Sayana, 2005; Lam, 2000:23). Every test should be scheduled well in advance so that the necessary preparations can be completed. Hiles & Barnes (2001:244) propose the completion of both component testing (a narrowed focus to test specific components of the overall plan) and comprehensive testing (a complete test of the all the plans executed in parallel with each other), both on-site and off-site. Testing is usually done through the simulation of a service interruption but often, through invocation and controlled execution, organisations invoke a specific disruption to check the validity of the plan. After the completion of the testing, the results should be communicated back to the appropriate parties to identify areas of improvements. The frequency of testing should be dependent on changes of business processes, technology,

business continuity management owners or any likelihood of a disruption materialising.

Once the testing has been completed, the plans should be communicated and distributed to the appropriated parties in the organisation. Hiles & Barnes (2001:37) suggest that organisations keep record of the plans distributed with the goal of simplifying the retrieval process of outdated versions. The parties should at the very least be aware of their role and responsibilities as detailed in each plan. However, to ensure the successful execution of the plans, the parties should ideally receive formal training on their business continuity management role and responsibilities. The importance of business continuity management training and awareness is supported by various literature sources, e.g. Manning (1999:244), Sayana (2005) and Doughty (2002) who explain that it forms an important part of the organisation's response procedures.

6.3.5 POST RESUMPTION REVIEW

The post resumption review detailed objective is applicable once an organisation has recovered from a disruption. The post resumption review objective aims to analyse the reports generated during the recovery process and to update the business continuity plan accordingly. In addition, Lam (2000:24) suggests that the plan should not only be updated after a disruption. The business continuity management plan should also be updated during the organisation's change management process, which is discussed in the subsequent sections. The different steps of the detailed objective, as interpreted through the content analysis, are presented in Figure 20.

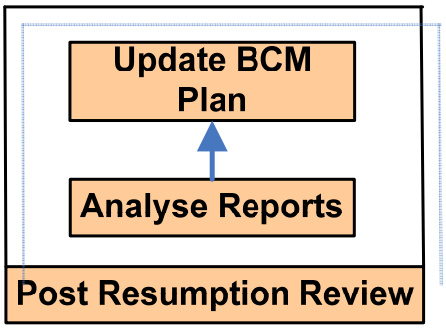

Figure 20: Business Continuity Management Detailed Objective - Post Resumption Review

6.3.6 PROJECT MANAGEMENT

Project management forms an important part in the assurance that the different detailed objectives of business continuity management get implemented correctly. Hiles & Barnes (2001:94) recognise the importance of project management within business continuity management and emphasise that it is not a once-off process. The detailed objective consists of a project management methodology that needs to be specified of which PMBOK is one example. Once chosen, this methodology is used develop a project plan that stipulates the implementation and revision of specific business continuity management detailed objectives. The detailed objectives covered in the project plan are aligned with the different components of the business continuity management framework and includes the management of critical organisational resources, management of risks, establishment of business continuity management guidelines and the development and implementation of a business continuity plan. This scope, together with the overall importance of project management when implementing business continuity management, is recognised by Doughty (2002). Lam (2000:20) explains that in addition to the selection of a project management methodology and plan, the project management objective must also identify the business and technical stakeholders together with the establishment of a business continuity management workgroup. These roles and groups are discussed in more detail in the roles section presented later in this chapter. The two steps of the project management detailed objective are presented in Figure 21, as identified through the content analysis.

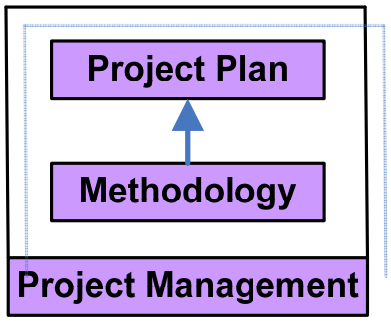

Figure 21: Continuity Detailed Objective - Project Management

The project management detailed objective is only applicable during the design and implementation of the business continuity management framework. Once completed, the maintenance of the framework should be a daily managerial responsibility.

6.3.7 CHANGE MANAGEMENT

The detailed objective of change management is present in all business continuity management initiatives with the exception of the auditing detailed objective. Figure 22 details the continuous process of incorporating changes in the business environment through business continuity management, as interpreted through the content analysis. The content of every business continuity management detailed objective should be aligned with any developments in the different areas of the organisation by means of change management. As stated by Sayana (2005), business continuity management should be synchronised with the actual environment of the organisation. Graham & Kaye (2006:327) warn that many organisations only update their business continuity management plan after a disruption, causing the plan to be outdated and inadequate. The goal of change management is to implement these changes in a controlled manner and to recognise the consequences it might have on the rest of the organisation. Similarly, the same change management practices should be applied when maintaining any of the business continuity management detailed objectives. Hiles & Barnes (2001:259) emphasise the importance of ensuring that change management activities do not change the strategies, approaches and underlying objectives defined by the organisation. In an attempt to make the plans as

comprehensive as possible, business continuity managers often get so involved in the detail that they sometimes diverge from the defined strategies.

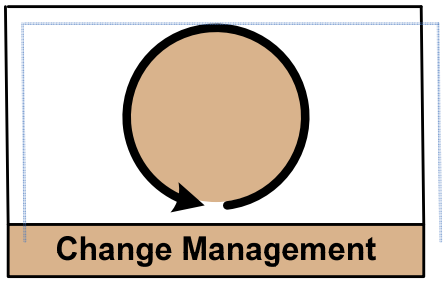

Figure 22: Continuity Detailed Objective - Change Management

6.3.8 AUDITING

Similar to change management, auditing should be present in all areas in business continuity management. Hiles & Barnes (2001:231) describe auditing as the writing of reports that documents and evaluates the organisation's environment with the goal of ensuring continuous readiness and relevance of an organisation's business continuity management plan. Calderon (2003:20) believes that the anticipated success of an organisation's business continuity management plan can be determined by performing regular audits. Rutherford *et al.* (2002:4) mention that audits on the implementation of compulsory business continuity management activities, as proposed by government legislations and regulations, can highlight inadequacies of the plan. Internal audits should be conducted on a regular basis and well in advance to external audits (Graham & Kaye, 2006:339). Sayana (2005) proposes the completion of internal audits on a quarterly basis and a comprehensive formal audit at least annually. When auditing a business continuity management plan, Hiles & Barnes (2001:232) remind organisations to also conduct off-site auditing and not only on-site auditing. The results of these audits should be evaluated and the necessary updates need to be implemented and incorporated in the business continuity management plan through the organisation's change management process. Figure 23 illustrates the continuous and all-inclusive characteristic of the auditing activities, as interpreted through the content analysis.

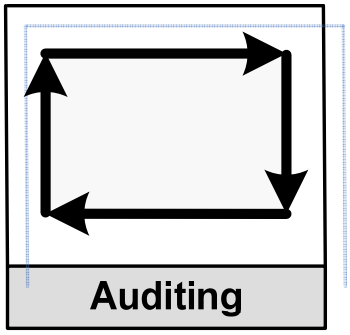

Figure 23: Continuity Detailed Objective - Auditing

6.4 BUSINESS CONTINUITY MANAGEMENT ROLE PLAYERS

The results obtained of the content analysis identified the different roles required to successfully practise business continuity management. The comprehensive list is indicated in Figure 14 and includes amongst others executives, boards and committees. Supporting these results, Graham & Kaye (2006:75) recognise the roles to be at an executive level, which include the chief executive officer (CEO), chief financial officer (CFO) and the chief information officer (CIO). At the very top is the CEO who has the ultimate responsibility of business continuity management. Reporting to the CEO are the CIO and CFO. The CFO is responsible for ensuring that the organisation has the financial resources to survive serious business interruptions. In addition, the CFO must ensure financial support is available to fund business continuity management initiatives. As business continuity management expenditures deliver no immediate return on investment, it is often difficult to obtain the financial support needed to implement it (Hiles & Barnes, 2001:363). More on the funding of business continuity management is presented in subsequent chapters. As mentioned previously, business continuity management has a strong focus on IT. For this reason, the CIO plays a prominent role in the assurance of business continuity, at least from an IT perspective. Under the CIO is the head of development, head of operations, chief architect and the head of IT administration. The head of development must ensure the implementation of the business continuity management detailed objectives. The head of operations is responsible for ensuring that the continuity initiatives get executed on a day-to-day basis. The chief architect has the responsibility of ensuring that the business

continuity management detailed objectives are designed in a scalable fashion that is integrated with the rest of the organisation. The head of IT administration is responsible for the coordination and supervision of business continuity management.

These role players are assigned to specific groups and committees that should be created in the organisation. The business continuity management board is responsible for initiating all business continuity management activities. A representative of the business continuity management board must be present in the project management office (PMO). The PMO should prioritise and schedule the different business continuity management tasks. The business continuity management steering committee is the driving force of the implementations and consists of a group of personnel who is accountable for specific deliverables. These personnel range from senior managers to managers, team leaders, supervisors and business owners. Lam (2000:21) agrees that a business continuity manager is responsible for assembling a team to execute the decisions made by the business continuity management steering committee. This manager should present key decisions to business owners and should lead them during the recovery processes if a disruption has occurred.

From the interpretation of the content analysis, it is clear that the organisation's executives should drive business continuity management. Business continuity management should be implemented throughout the organisation on all levels, resulting in the entire organisation's personnel to be involved in business continuity management.

6.5 INTEGRATING BUSINESS CONTINUITY MANAGEMENT WITH THE COBIT AND ITIL IT GOVERNANCE FRAMEWORKS

The result of the content analysis identified various inputs and outputs of business continuity management, as indicated in Figure 15. The inputs and outputs are categorised according to the two IT governance framework used during the content analysis namely COBIT and ITIL. Business continuity

management can be tightly integrated with the two IT governance frameworks by means of these inputs and outputs.

Each COBIT control objective and ITIL process element is discussed according to the relationship it has with business continuity management. These discussions are based on the literature survey on these IT governance frameworks. Figure 24 presents the COBIT control objectives that relates to business continuity management, whereas Figure 25 details the ITIL process elements that serve as business continuity management inputs and outputs.

By illustrating the relationship that business continuity management has with other IT governance processes, organisations can easily integrate the business continuity management framework developed in this research with their COBIT and/or ITIL IT governance framework.

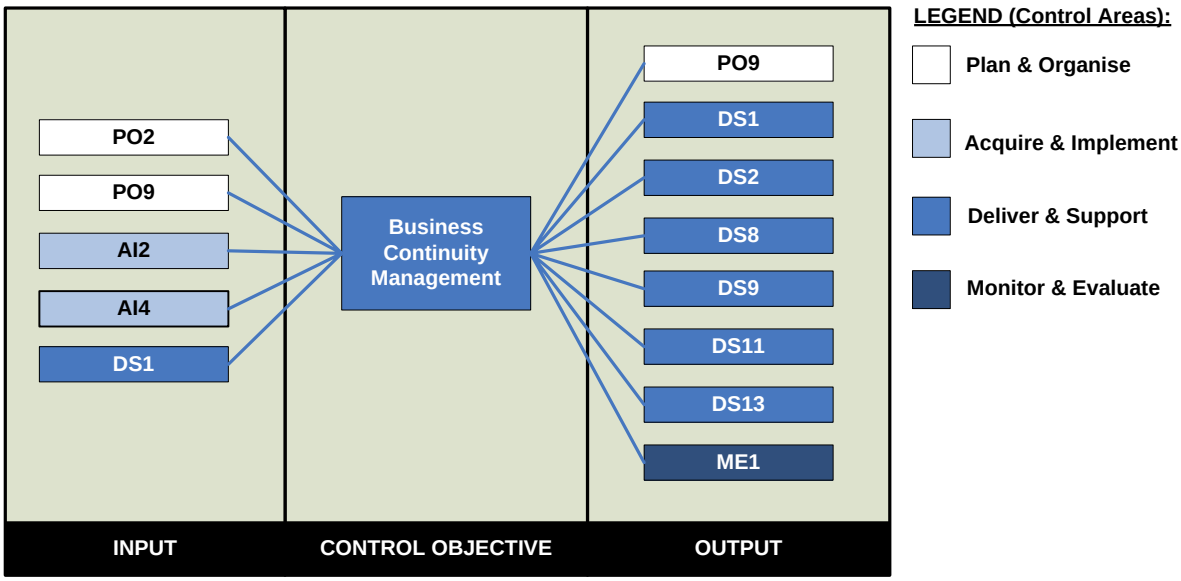

Figure 24: Business Continuity Management Inputs and Outputs According to COBIT

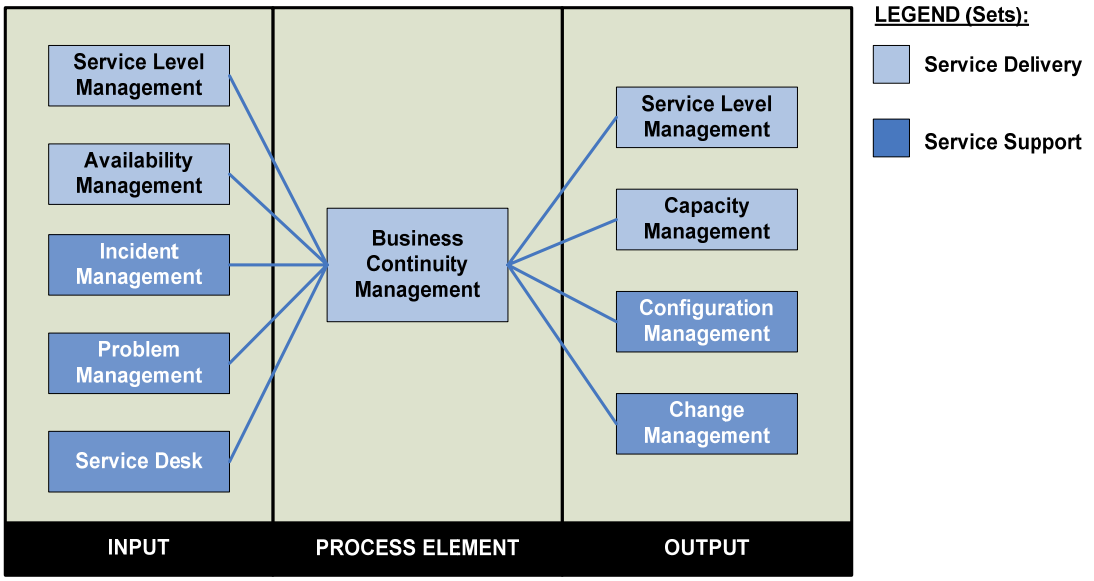

Figure 25: Business Continuity Management Inputs and Outputs According to ITIL

6.5.1 COBIT INPUTS

Business continuity management has five COBIT inputs namely AI2, AI4, DS1, PO2 and PO9. The business continuity management inputs are from three COBIT control areas: Plan & Organise, Acquire & Implement and Deliver & Support. The forth control area, Monitor & Evaluate, does not provide any inputs to DS4. Both PO2 and PO9 are control objectives from the Plan & Organise control objective area, objectives AI2 and AI4 are from the Acquire & Implement control objective area and DS1 is from the Deliver & Support control objective area.

6.5.1.1 PO2 – DEFINE THE INFORMATION ARCHITECTURE

The PO2 control objective is also known as 'Define the Information Architecture. The objective of PO2 is to establish an enterprise information model where data can seamlessly be stored, manipulated and retrieved by different applications to facilitate the business processes of an organisation. Amongst the detailed control objectives of PO2, the most important objective relating to business continuity management is data classification. Data classification analyses the criticality and sensitivity of data and creates a scheme accordingly. Typically the scheme includes data ownership, data retention and retirement, but most importantly data security. Data security

stipulates the different user categories and the data access rules used by each category to access a particular data security level.

6.5.1.2 PO9 – ASSESS AND MANAGE RISKS

PO9 is dedicated to the risk assessment and management activities in an organisation. The risk management framework identifies and analyses risks in an attempt to minimise the probability and impact of the risk on the organisation. The detail objective of PO9 that provides input to business continuity management is the assessment of risks. Risk assessment includes the calculation of the risk materialisation probability and an impact analysis study. The business impact analysis should be done on an individual, category and portfolio basis.

6.5.1.3 AI2 – ACQUIRE AND MAINTAIN APPLICATION SOFTWARE

Dedicated to the acquisition and maintenance of software, AI2 aims to provide the organisation with applications to support their business operations while ensuring that it is cost effective, timely and of sufficient quality. Business continuity management relies heavily on the output of AI2, specifically on the availability, continuity and recovery specification. The availability specification details the application dependencies. Business critical functionality and the risks introduced during the utilisation of the application are documented in the business continuity management specification. Closely related, is the recovery specification that stipulates the response actions to follow should the availability of the application be disrupted.

6.5.1.4 AI4 – ENABLE OPERATION AND USE

The operation and usage of organisational applications enable the applications to become a facilitator for business processes. The AI4 control objective aims to transfer knowledge on acquired applications to different types of users by means of documentation and training, hence enabling the integration of the IT infrastructure and business processes. Business

continuity management is supported by AI4, by means of the user, operational, support, technical and administrator manuals. Manuals should be comprehensive enough so that it can support training activities and assist the daily troubleshooting of the different application audience to ensure the continuity of business processes.

6.5.1.5 DS1 – DEFINE AND MANAGE SERVICE LEVELS

The responsibility of defining and managing service level agreements is assigned to the control objective of DS1. DS1 is dedicated to the identification, agreement and monitoring of IT service levels that should be aligned with business strategy. The detailed objective of developing a service level management framework, specifically the component focussing on service level agreements (SLA), is important to the continuity of an organisation. Items contributing towards the success of SLA's are accessibility, reliability, performance, capacity planning, supporting levels and security.

6.5.2 ITIL INPUTS

All the ITIL inputs to business continuity management is categorised into two ITIL sets namely Service Delivery and Service Support. Service Level Management and Availability Management are process elements under the Service Delivery set, whereas the Incident Management, Problem Management and Service Desk process elements are components of the Service Support set. Each of these process elements is now broadly discussed.

6.5.2.1 SERVICE MANAGEMENT

Service level management (SLM) is responsible for managing IT service levels required by the organisation to function effectively and efficiently. By means of service level agreements (SLA), SLM improves the quality of an organisation's IT services. SLA's detail service objectives and responsibilities

between a third-party service provider and a customer. The SLM detailed control objective is critical to the business continuity of an organisation. An important element of SLM is the SLA's with third party service providers that specifically contributes to the continuity of an organisation. These SLA's should be identified and categorised as to be included in the business continuity framework.

6.5.2.2 AVAILABILITY MANAGEMENT

The interdependency of the business and IT infrastructure of modern organisations implies that the business operations will become unavailable should an organisation's IT infrastructure become unavailable. Availability management is dedicated to the continuous availability of an organisation's IT infrastructure and consequently also services. Business continuity management and availability management is not alike even though they share a very strong relationship. Availability management provides key inputs to business continuity management. Whereas business continuity management is responsible for business resumption after a disruption, availability management focuses mainly on the availability of an organisation's IT services. The input which availability management provides to business continuity management is specifically aimed at the continuity of IT services by reducing the risks associated with service downtime. As this can be considered to be a subcomponent of business continuity management, the strong relationship between business continuity management and availability management is evident.

6.5.2.3 INCIDENT MANAGEMENT

Incident management aims to restore disrupted services while minimising the impact it has on business operations. Incident management is practiced by an organisation's service desk through a set of known errors and solutions. Should a problem fail to be resolved by the service desk, the problem will be directed to problem management. Another use of incident management is to restore a service as soon as possible, often resulting in workaround solutions.

Reports on the incidents registered are often used as input to business continuity management to improve the business continuity management initiatives of an organisation. If an organisation can decrease the number of incidents, the continuity of the organisation will improve as a result of the decrease in service downtime.

6.5.2.4 PROBLEM MANAGEMENT

Similar to incident management, problem management aims to restore disrupted services while minimising the impact it has on business operations. Problem management differs from incident management in the sense that problem management only handles calls which could not be resolved by the service desk. In addition, problem management attempts to identify permanent solutions to incident management workarounds by resolving the root cause of the problems. Once problem management has resolved a problem, the error details and diagnosis is stored in the know error database to become part of incident management as practiced by the service desk. The relationship that business continuity management has with problem management is similar to that of incident management. Reports generated from problem management will identify possible problem areas in the organisation and can also be used to implement preventive measures, therefore improving the continuity of the organisation.

6.5.2.5 SERVICE DESK

The service desk of an organisation acts as a central point that is continuously available for internal and external users to communicate and resolve issues related to the organisation. The service desk replaces the traditional help desk – which only focused on the logging of incidents and requests – to also include the handling of client liaison. The relationship between the service desk and business continuity management is of extreme importance. The service desk's reports and statistics on services, specifically those reported by incident and problem management, often proactively identifies and prevent disasters from materialising.

6.5.3 COBIT OUTPUTS

The outputs of business continuity management that relates to other COBIT control objectives are mainly focused on the Deliver & Support control area, specifically DS1, DS2, DS8, DS9, DS11 and DS13. Aside from those, the outputs of business continuity management also act as inputs to PO9 from the Plan & Organise control area and ME1 from the Monitor & Evaluate control area. Control objectives DS1 and PO9 services as both inputs and outputs to business continuity management, however, the detailed control objectives on which these inputs and outputs are based, differs. The result of business continuity management does not influence any of the control objectives dedicated to the Acquire & Implement control area.

6.5.3.1 PO9 – ASSESS AND MANAGE IT RISKS

PO2 is one of the two control objectives which servers as both input and output to business continuity management. As stated in the input section, PO9 aims to recognise, assess and minimise the potential impact which IT risks can have on the business processes of an organisation. The detailed control objectives of PO9 are discussed on a high level in the COBIT input section of business continuity management. The output of business continuity management serves as input to PO9. Specifically, the output includes the testing results of the business continuity management plan. The results of the testing could indicate whether the IT risks assessed in the risk management framework are not only comprehensive and correct, but also whether the testing identified new risks.

6.5.3.2 DS1 – DEFINE AND MANAGE SERVICE LEVELS

The Define and Manage Service Levels (DS1) is the second control objective that acts as both an input and output to business continuity management. As stated previously, the input of DS1 emphasises the importance of SLA's and OLA's towards the continuity of an organisation. DS1's control objectives are briefly presented in the COBIT input section of business continuity

management. The output of business continuity management has a clear relationship with the input of DS1: After the analysis objective of business continuity management, specifically those aimed at disaster recovery, new services might be required by the organisation. After business continuity management has highlighted new service requirements, DS1 is responsible for defining and managing each service together with the roles and responsibilities associated with the service.

6.5.3.3 DS2 – MANAGE THIRD PARTY SERVICES

The management of third party services is dedicated to the DS2 control objective. DS2 aims to ensure that the third party services utilised by an organisation are cost effective and beneficial to business requirements – all whist risks are being balanced. The assurance of business continuity can result in the identification of new services. If these services cannot be provided by the organisation, it is often outsourced to third parties. Specifically, disaster recovery services, together with the associated roles and responsibilities, are often identified during the implementation of business continuity management.

6.5.3.4 DS8 – MANAGE SERVICE DESK INCIDENTS

The service desk acts as the first line of communication between the customer and the organisation. An organisation's service desk is critical to the timely and accurate response of employee and customer communications such as enquiries and incident reporting. In addition, all communications also need to be analysed to identify trends. The service desk implemented through DS8 allows an organisation to identify the materialisation of any incidents or disasters. Business continuity management specifies the thresholds for both incidents and disasters. Should the service desk or trend analysis indicate that these thresholds have been exceeded, the business continuity management plan gets activated.

6.5.3.5 DS9 – MANAGE THE CONFIGURATION

Configuration management focuses on the configuration of hardware and software through the utilisation of a configuration repository. During the configuration management process, the criticality of IT configuration items should be identified and specified. Each configuration item has to be prioritised according to the specifications detailed in the business continuity management framework.

6.5.3.6 DS11 – MANAGE DATA

The eventual goal of data management is to provide an organisation with accurate information in a timely and secure manner. DS11 focuses on managing a media library, the backup and recovery of data and the identification and implementation of new data requirements. In support of various business functions, organisations create, retire and manipulate data on a daily basis. Data often gets transformed to information, which supports business decision making. It is evident that the continuity of an organisation is dependant on the data of the organisation. For this reason, the detailed control objectives dedicated to the storage, backup and protection of data are dependant on the business continuity management requirements.

6.5.3.7 DS13 – MANAGE OPERATIONS

DS13 describes the management of operations that aims to supervise the execution of daily business operations in an organisation. Specifically, DS13 aims to guarantee data integrity and ensure the availability of an organisation's IT infrastructure. The management of operations is applicable to all resources in the organisation (applications, information, infrastructure and people). Similar to DS11, DS13 utilises the output of business continuity management during the establishment of a backup storage and protection plan. In addition, DS13 contributes towards business continuity management through the preventive hardware maintenance detailed control objective to reduce hardware failures and to minimise the impact of a disruption.

6.5.3.8 ME1 – MONITOR AND EVALUATE IT PERFORMANCE

The ME1 control objective is dedicated to the evaluation of IT performance though a defined monitoring and reporting process. Monitoring is done to ensure that the organisational activities are aligned with policies, strategies and governance compliances. The continuous monitoring of IT performance is critical to the sustainability of an organisation. Business continuity management stipulates which elements of the IT infrastructure should be measured. The monitoring and reporting of IT performance is important to identify any malicious disasters in a timely fashion in an attempt to minimise the impact it might have on the organisation. Additionally, the assessment of IT performance can also highlight trends of business continuity disturbances and possibly also the root causes. In return, this information can be used to rectify and improve the continuity of an organisation.

6.5.4 ITIL OUTPUTS

Similar to the ITIL inputs to business continuity management, the outputs are also limited to the Service Delivery and Service Support ITIL sets. Service Level Management is the only process element which acts as both input and output to business continuity management. Together with Capacity Management, they are the only two process elements from the Service Delivery set. From the Service Support set, both the Configuration Management and Change Management process elements utilises the output of business continuity management as inputs.

6.5.4.1 SERVICE LEVEL MANAGEMENT

Service level management serves as both input and output to business continuity management. Service level management aims to establish IT services both external to the organisation (by means of SLA's) and internal to the organisation (by means of OLA's). The detailed objectives of SLM are presented in the business continuity management input section. To recall, the SLM input to business continuity management is about identifying business critical IT services and to include them in any business continuity management initiatives. Additionally, the ITIL output of business continuity

management also acts as input to SLM. The business continuity management framework will most likely introduce new IT services to the organisation and most definitely require new third party services to support business continuity management.

6.5.4.2 CAPACITY MANAGEMENT

Capacity management is responsible for ensuring that the business demands of an organisation's resources are met, specifically those related to the IT infrastructure. Capacity management aims to justify the cost of capacity expenditures while maintaining a balance between supply and demand. Capacity management consists of business, service and resource capacity management. The goal of business capacity management is to make provision for future business requirements like new developments and improvements of existing IT services. Service capacity management identifies the minimum resources required to deliver these services and ensure that the OLA's and SLA's are met despite of peaks and troughs. Lastly, resource capacity management accurately manage each of the resources with the organisation in accordance with the minimum specification, as determined by service capacity management. The output of business continuity management details the minimum capacity required to restore business activities to an operational state after a disruption. The capacity specifications that are required to successfully perform the recovery processes should also be clearly stipulated in the business continuity management requirements.

6.5.4.3 CONFIGURATION MANAGEMENT

The goal of configuration management is to economically manage the information needed to implement an organisation's IT infrastructure centrally and with sufficient quality. Configuration management is based on an application that interacts with the configuration management database (CMDB) to manage configuration items effective and efficiently. The relationship between business continuity management and configuration

management mainly focuses on storing the particulars of the different IT infrastructure items critical to the continuity of an organisation. This information not only includes the configuration details of each item, but also additional information such as the technical specification and supplier details.

6.5.4.4 CHANGE MANAGEMENT

Change management aims to ensure that all changes are implemented with minimal costs, risks, disruption and impact on IT services through the use of predefined policies and procedures. Change management activities are often initiated whenever business continuity management plans are updated. Often change management activities are initiated based on the results obtained from detailed business continuity management objectives (specifically risk assessment) in an attempt to improve the sustainability of an organisation. Any changes in the organisation's environment should also be updated in the business continuity management initiatives through official change management activities.

6.6 CONCLUSION

This chapter presented the interpretation of the results obtained from the content analysis. These interpretations where categorised according to the objectives and detailed objectives of business continuity management, the role players responsible for business continuity management and the relationship that business continuity management has with COBIT and ITIL. The interpretations were based on the results of the content analysis represented by the following figures: Figure 12, Figure 13, Figure 14 and Figure 15. Where possible, academic references to support the interpretations were also included.

According to the content analysis, the discontinuity of an organisation can be caused by the materialisation of a risk, threat or event. Business continuity management should analyse the impact which potential disruptions might have on an organisation and implement preventive and responsive plans for

each instance. The detailed objectives of business continuity management are resource management, risk management, business continuity management guidelines development, business continuity management plan development, post resumption review, change management, project management and auditing. To ensure the effective and efficient implementation and management of these objectives, an organisation must have a well-formulated managerial structure with defined roles and responsibilities. In addition, the organisation must also have specific boards, groups and committees with the goal of directing business continuity management. Lastly, the interpretation of the content analysis also identified the various relationships that business continuity management has with the other control objectives of COBIT and process elements of ITIL. By presenting these relationships, organisations can easily integrate business continuity management with the COBIT and ITIL IT governance frameworks to ensure, amongst others, IT continuity.

In the following chapter, the details of the empirical study are presented. This includes the interview questions, participant details and the conclusions interpreted from the empirical study.

CHAPTER 7
EMPERICAL STUDY DETAILS AND FINDINGS

7.1 INTRODUCTION

The empirical part of this study aims to complement the information derived from the literature survey and content analysis. The empirical study consists of interviews with selected practitioners who have relevant experience in the areas of business continuity management and IT governance.

This chapter presents the results of each of the interviews with the participants. The chapter also includes the background of each participant, together with a high level overview of the organisation each participant represent. The main part of this chapter is dedicated to the interpretation and documentation of the participants' opinions on the various subjects related to this research.

7.2 EMPERICAL STUDY DETAILS

The prerequisite for the selection of these practitioners was for them to have expertise in the area of business continuity management and IT governance. In cases where individuals only had expertise in one particular area, an additional participant (who was an expert in the other area) was identified in the same organisation. The results presented in this chapter are according to the viewpoint of the different organisations and not per individual participant.

The empirical study obtained information from these practitioners by means of interviews. The goal of the interviews was to gain an understanding of each practitioner's organisation and the role they play in the area of business continuity management and/or IT governance. More importantly, the questions posed to the different organisations were aimed at identifying their perceptions on business continuity management through the viewpoint of IT governance.

7.2.1 INTERVIEW QUESTIONS

The questions posed to the participants were categorised into two sections. The first section focused on the participant and the organisation represented by the participant. The second section was dedicated to obtaining an understanding about the individual's perceptions on business continuity management and IT governance.

In the first section, the organisation represented by the participants was discussed together with the position of the participants(s) in the respective organisation. The business continuity management and IT governance initiatives of the organisation, together with the manner in which these participants have been involved in these initiatives, were also examined.

The second section focused on the objective of business continuity management and IT governance as well as the evolution of both areas. The relationship and integration between business continuity management and IT governance were also explored. Specific points about business continuity management were examined which includes the role players involved as well as the main challenges and detailed objectives of business continuity management.

The remaining part of this chapter presents the conclusions derived from the interviews, grouped under the different discussion points.

7.2.2 BACKGROUND OF PARTICIPANTS

The following section presents a background on the participants and the organisations represented by them. Due to the confidentiality of the interviews, the identities of the four companies included in this research is notated using A, B, C and D. The participants are referred to as Participant A1, A2, B1, etc. where the first character represents the organisation and the second character represents the participant number.

7.2.2.1 ORGANISATION A

Organisation A is a South African government department that plays a critical role in the economy of South Africa. In recent years organisation A has been praised by the press for its world-class technology implementations. This has resulted in organisation A being one of the most technologically advanced government institutions in South Africa. One of the main purposes of organisation A is to provide continuous services to the country's citizens, which have a direct impact on the finances of South Africa. This activity and many more is directly dependant on the institution's IT infrastructure.

Organisation A utilised the services of consultants at different stages of the initial business continuity management and IT governance framework implementations. At the time of the interview, organisation A had implemented a business continuity management and IT governance framework. These implementations have matured over years and are continuously being maintained and improved by organisation A.

Organisation A's participant is responsible for managing all business continuity management and IT governance activities. This includes the design, implementation and management of all activities related to business continuity management and IT governance.

7.2.2.2 ORGANISATION B

Organisation B is one of the main global consulting firms with offices in South Africa. This organisation has an excellent reputation for delivering advisory services to clients with a specific focus on auditing and business processes. The interview conducted with organisation B focused on their services to clients and not the implementations in the organisation itself.

Organisation B is regarded as an industry leader in the area of governance and has proposed, developed and implemented both business continuity management and IT governance world-wide. Different work streams in the

organisation have specific areas of expertise of which business continuity management and IT governance are two examples.

Two participants from organisation B were approached. Participant B1 is an expert in the area of business continuity management whereas participant B2 has expertise in the area of IT governance. Even though each participant has a particular area of proficiency, both participants are well educated and experienced in business continuity management and IT governance.

7.2.2.3 ORGANISATION C

Organisation C is one of the world's largest ICT service providers and has offices in 23 countries world wide - consisting of 52,000 employees in total. This organisation offers consulting and outsourcing services to 160,000 multinational clients and supports a global network, spanning 40 countries. Organisation C offers 'one stop ITC solutions' consisting of a number of services, including software development and maintenance and the management of their clients' IT infrastructures.

Organisation C has exceptional experience in business continuity management and IT governance as they have implemented both areas at a number of enterprise clients both locally and internationally. In addition to this, organisation C has also reached (to their opinion) a level of maturity in the implementation of business continuity management and IT governance. Both the COBIT and ITIL frameworks are used by organisation C as IT governance frameworks.

Two participants from organisation C were interviewed. Participant C1 is a specialist in the area of business continuity management and is, amongst others, responsible for the continuity of the organisation's local offices. This participant has also been consulted by clients to define and manage business continuity management projects. Participant C2 is a professional in the field of IT governance and plays an active role in the IT governance initiatives of

the organisation's local branches. Similar to participant C1, participant C2 also offers his expertise to clients in the form of executive consulting.

7.2.2.4 ORGANISATION D

Organisation D is another leading South African consulting firm and is also represented globally. With more than 133,000 employees, organisation D operates in 110 cities in 48 countries. Organisation D offers a variety of services in different industries including communication, technology, financial, products, resources and government. These services range from high value consulting to implementation and support.

Many business continuity management and IT governance projects have been implemented globally by organisation D. In many cases, organisation D makes use of a global knowledge base and international expertise to ensure the professional delivery of local projects. Organisation D is also of the opinion that the business continuity management and IT governance initiatives implemented in their environment is of a world class standard.

Organisation D's participant has extensive knowledge in the area of business continuity management. Participant D1 has been organisation D's global asset protection lead for over six years, specifically in the area of business continuity management. The participant has also provided consulting services globally. In addition, participant D1 has experience in IT governance even though he does not consider himself to be an IT governance specialist.

7.3 EMPERICAL STUDY FINDINGS

The response of the different participants is presented in the following sections. The results of the interviews are categorised according to the research topics.

7.3.1 THE OBJECTIVE OF BUSINESS CONTINUITY MANAGEMENT

All four organisations define the objective of business continuity management as the managerial activities to ensure an organisation can successfully recovery after a disruption. Organisations A, C and D differentiate between the continuity of an organisation's IT infrastructure and business operations. Business continuity management covers all aspects of an organisation specifically business processes, whereas disaster recovery is specifically dedicated to the continuity of an organisation's IT infrastructure. Organisation C is the only organisation to specifically mention that disaster recovery is a subcomponent of business continuity management. All four organisations emphasises the importance of a business continuity management framework aimed specifically at developing preventive and responsive plans.

The findings of the objective of business continuity management according to the empirical study are consistent with the results obtained from the literature survey and content analysis. Business continuity management aims to prevent disruptions in an organisation and to restore business operations should a disruption occur. It does so by following predefined plans. Business continuity management is focused on business continuity whereas disaster recovery is dedicated to IT continuity.

7.3.2 THE OBJECTIVE OF IT GOVERNANCE

Organisation's A, B and C describe IT governance in a consistent manner: IT governance is aimed at aligning IT initiatives with business objectives to support the strategic goals of an organisation. Organisation D places more emphasis on the fact that IT governance introduces specific IT standards and best practices in the organisation. Organisation B, C and D explain that IT governance is aimed at executives like the CEO and CIO. The ability of IT governance's to manage risks in an organisation is only recognised by organisation A. All four organisations agree that IT governance should be implemented by means of a formal IT governance framework such as COBIT and ITIL.

The manner in which the participants define the objective of IT governance is similar to the literature survey. IT governance is the strategic alignment of IT initiatives with business operations and is usually the responsibility of the CIO.

7.3.3 EVOLUTION OF BUSINESS CONTINUITY MANAGEMENT AND IT GOVERNANCE

All four organisations are of the opinion that traditionally business continuity management mainly focused on IT. In recent years, the scope of business continuity management has increased to place more emphasis on business processes. This has resulted in the traditional technology focus of business continuity management to be replaced with disaster recovery. Organisation D believes that modern business continuity management consists of various subcomponents focusing on specific areas in the organisation of which disaster recovery is one example. Organisation C is of the opinion that an increasing number of organisations have moved the responsibility of ensuring the organisation's continuity from the IT department to business owners. The evolution of business continuity management is, according to organisation C, party as a result of government regulations and legislations. The influence that risk management had on the evolution of business continuity management is only recognised by organisation D. According to organisation D, risk management has increased the scope of business continuity management to include all aspects of an organisation

According to organisation A, IT governance has become increasingly important over the past couple of years as a result of additional laws and compliance regulations. Organisation B explains that IT governance has come focused on supporting business processes. The auditing of these frameworks has also become extremely important as it ensures the quality of implementations and the compliance with industry standards. Organisation C and D is of the option that IT governance has migrated IT management from a technical level to an executive level with a strong business focuses. Consequently, IT governance has since evolved from an IT related background initiative to an integrated business enabler and value deliverer.

The empirical study indicates that both business continuity management and IT governance have evolved from being technology oriented to being business oriented. These findings are in line with the results of the literature survey.

7.3.4 RELATIONSHIP BETWEEN BUSINESS CONTINUITY MANAGEMENT AND IT GOVERNANCE

Organisation A and D conceptualise disaster recovery as a subcomponent of business continuity management, which is in its turn a subcomponent of risk management. Risk management and IT governance are both subcomponents of corporate governance. IT governance (specifically COBIT) does not adequately cover business continuity management. Therefore, even though a relationship between business continuity management and IT governance exists, IT governance has a stronger relationship with disaster recovery. Organisation A and B therefore have two areas of focus: the business continuity management section that is implemented across all sections of the organisation and disaster recovery that is implemented only in the IT departments. Within these IT departments, IT governance is also implemented and hence the direct relationship between IT governance and disaster recovery.

Organisation B explains that business continuity management is a subcomponent of risk management and that risk management is one component of corporate governance. Risk management and subsequently business continuity management should not be implemented horizontally in an organisation, but rather vertically in order to cover specific sections of different governance areas. This proposal has the implication that business continuity management is a subcomponent of IT governance and that this particular instance of business continuity management specifically focuses on IT. In a similar way, business continuity management is vertically present in financial governance and specifically focuses on the financial continuity of an organisation. Figure 10 in chapter four illustrates the typical horizontal relationship between business continuity management and IT governance as

described by the literature, whereas Figure 26 demonstrates organisations B's proposal of a vertical relationship. However, organisation B also acknowledges that disaster recovery is a subcomponent of business continuity management and has the specific goal of ensuring the continuity of an organisation's IT infrastructure.

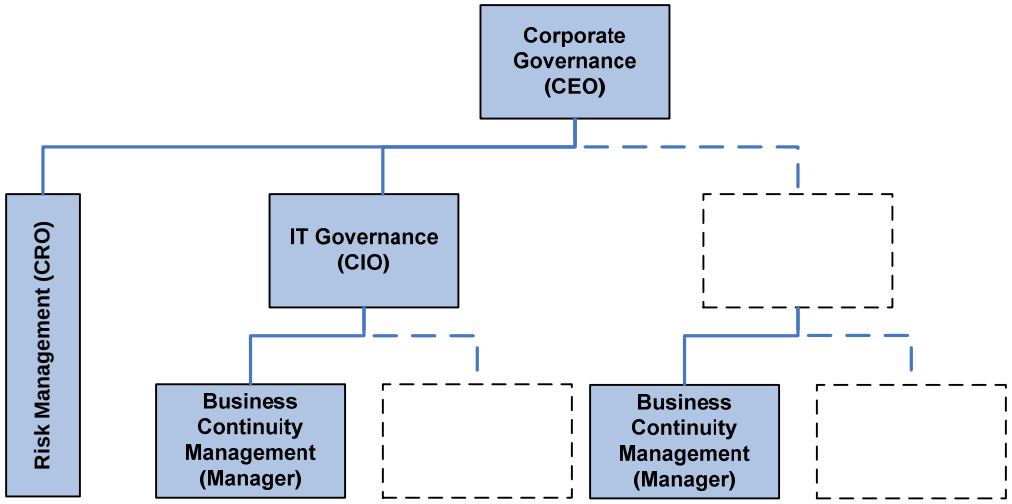

Figure 26: Organisation B's Vertical Alignment of Business Continuity Management and IT Governance

Organisation C proposes that the relationship between business continuity management and IT governance is a combination of what was proposed by organisation A and B. Both IT governance and risk management are subcomponents of corporate governance. Risk management consists of business continuity management, which is made of amongst others, disaster recovery. As proposed in Figure 26, risk management should be implemented vertically in an organisation. The difference between organisation C's approach is that IT governance has a stronger focus on disaster recovery and not business continuity management, even though disaster recovery is a subcomponent of business continuity management. For the remaining subcomponents of corporate governance, organisation C agrees that each component should manage their own business continuity while being centrally executed by risk management.

Based on these conclusions, the relationship between business continuity management and IT governance is clear. Organisation A's description of the

relationship between business continuity management and IT governance is similar to results obtained from the literature survey. Even though this relationship is not the same for each organisation, it is evident that corporate governance, risk management and disaster recovery play in important role defining the relationship between business continuity management and IT governance.

7.3.5 LEVEL OF INTEGRATION BETWEEN BUSINESS CONTINUITY MANAGEMENT AND IT GOVERNANCE

Organisation B and C promote a high level of integration between business continuity management and IT governance. These organisations specifically mention that practitioners should make use of COBIT's DS4 and ITIL's ITSCM, amongst others, as a guideline for the implementation of business continuity management and subsequently disaster recovery. However, organisation B and C also explain that the implementation of DS4 and/or ITSCM is not sufficient to ensure the continuity of an organisation. For this reason, these IT governance processes should be supplemented with additional business continuity management initiatives. Organisation A recognises the importance of integrating business continuity management and IT governance. However, in organisation A DS4 and ITSCM is part of the disaster recovery implementation, which is the responsibility of the IT department. Even though organisation D does not recognise any specific IT governance processes dedicated to business continuity management, the organisation believes that a comprehensive disaster recovery implementation should support a high level of integration between business continuity management and IT governance.

Organisations A, B and C mentions that certain IT governance processes, specifically COBIT's DS4 and ITIL's ITSCM, contribute towards the business continuity. These two processes were also identified in the literature survey and analysed in the content analysis.

7.3.6 ROLE PLAYERS OF BUSINESS CONTINUITY MANAGEMENT

All four organisations agree that the executives of an organisation should be responsible for business continuity management, which include the CEO, CIO, CRO and COO. The CEO has the ultimate responsibility of business continuity management. The CIO also plays an important role in assuring the organisation's IT continuity as he/she has the responsibility of managing disaster recovery. The COO focuses more on business operations and consequently business continuity management. The CRO and business continuity manager have a strong relationship and are responsible for the execution of business continuity management as implemented by the different organisational departments. The CRO must coordinate all risk management activities – like business continuity management – across the different areas of the organisation. These executives form part of a business continuity management committee, which is strongly propagated by organisation B and C. Organisation D also adds the role of the CFO, who is responsible for financial continuity, to the list of executes responsible for business continuity management.

Unlike the literature survey and content analysis, the empirical study identified an additional role player of business continuity management, namely the COO. The rest of the role players have all been identified by the literature survey and content analysis.

7.3.7 MAIN CHALLENGE FOR BUSINESS CONTINUITY MANAGEMENT

Organisations A, B and C recognise the process of obtaining funding as the foremost challenge of business continuity management. Organisations often find it hard to motivate and obtain budget for business continuity management implementations because it does not always deliver return on investment, Organisation A explains that it is challenging to find a balance between funding initiatives that are 'unlikely' to occur and initiatives that are 'more likely' to occur.

Organisation C also recognises the challenge of moving the responsibility of business continuity management away from the IT department and to the

relevant business department(s). Closely related to this, is another challenge mentioned by organisations A, namely the creation and maintenance of a relationship between the business continuity management department and the IT department responsible for disaster recovery. The dependency that a typical organisation's business processes have on IT makes it critical for these two departments to work closely together.

A different challenge is identified by organisation D, namely globalisation. It is challenging to implement business continuity management globally in a consistent, integrated and synchronised manner. When having international suppliers and clients, business continuity management becomes even more challenging. The final challenge, as mentioned by organisation D, is the skills and expertise required to create plans for business continuity management and the execution thereof. In addition, organisation A also identifies the updating and distribution of the business continuity management plan(s) as a very challenging task.

The empirical study clearly identified funding as the most challenging aspect of business continuity management. In addition to funding, practitioners also mentioned the shift of managing business continuity from the IT department to the business department(s) as very challenging. This is closely associated with the challenge of obtaining the relevant skills and expertise to execute business continuity management.

7.3.8 DETAILED OBJECTIVES OF BUSINESS CONTINUITY MANAGEMENT

The detailed objectives of business continuity management, as implemented by organisation A, are similar to the framework implemented by the Government of Saskatchewan as referenced by The Business Continuity Institute (The Business Continuity Institute, 2006). Graham & Kaye (2006:87) also propose the same framework for business continuity management. The framework is presented in Figure 27.

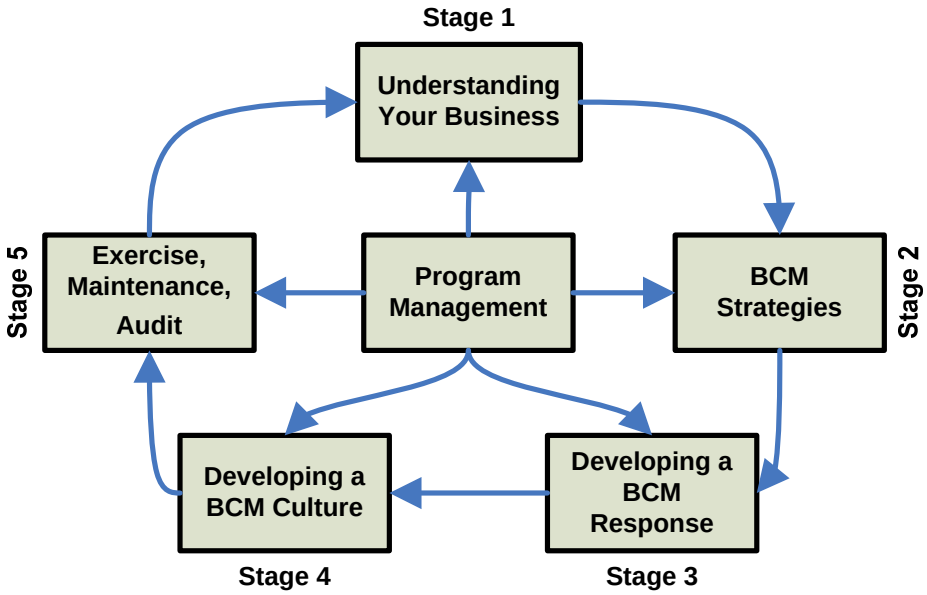

Figure 27: Government of Saskatchewan Business Continuity Management Framework (The Business Continuity Institute, 2006; Graham & Kaye, 2006:87)

In the centre of the framework is the business continuity management program. The program is dedicated to defining a business continuity management policy and strategy, managing business continuity activities and ensuring the organisation's readiness to respond to disruptions. Stage one is dedicated to understanding the organisation. This includes analysing the organisational strategy, conducting a business impact analysis and assessing and controlling risks. The next stage is about developing business continuity management strategies on an organisational, process and resource recovery level. Stage three develops a business continuity management response plan, which includes the managerial activities, public relationship management and media responses, amongst others. Stage four aims to develop a business continuity management culture by creating awareness, providing training and monitoring the business continuity behaviour of personnel. The final step is about testing, exercising, maintaining and auditing business continuity management activities.

The detailed objectives of business continuity management, as proposed by organisation B, were discussed on a very high level. The first step of business continuity management is the identification of critical business processes and the classification of the resources that support these

processes. The next step is to perform a risk assessment to identify the risks associated with each resource. Once the assessment is complete, a business impact analysis must be conducted. A framework should then be developed which documents, amongst others, the business continuity management strategies and approaches defined by the organisation. Based on the framework, a business continuity plan should be developed. The business continuity management plan consists of other plans like the a disaster recovery plan, emergency response plan, crisis management plans, response plan, resumption plan, public relations plan, etc. This plan should be tested on a regular basis and updated as the organisation's environment changes. The implementation of business continuity management needs to be managed like any other project, following a proper project management methodology and project plan.

Organisation C proposed that a business continuity management framework consists of four phases. Phase one is dedicated to achieving executive buy-in and establishing an awareness of the need for a business continuity management project. It includes the definition of a high level scope and possible project milestones. During phase two, a risk assessment must be conducted which makes use of pre-audits to identify existing vulnerabilities. This activity is complemented with a business impact analysis and based on the result of both activities, a business continuity management strategy is formulated. The initial stage of phase three consists of the development of a project plan. The project plan details the development and implementation process of business continuity management activities at managerial and departmental levels. Different plans must be developed to focus on specific areas in the organisation. One example of such an area is IT, in which case a disaster recovery plan must be developed. In addition to the plans, risk reduction measures must also be implemented. The final stage of the framework is the finalisation of the project. This includes the validation of the implementation activities against the defined strategies, education and establishment of awareness amongst the entire organisation and potential reviews to some of the plans. Testing also plays a critical role in the final phase. A post-audit should ideally be conducted to identify whether the

implementations have reduced the vulnerabilities identified during the risk assessment exercise.

The detailed objectives of a business continuity management framework as proposed by organisation D, is displayed in Figure 28.

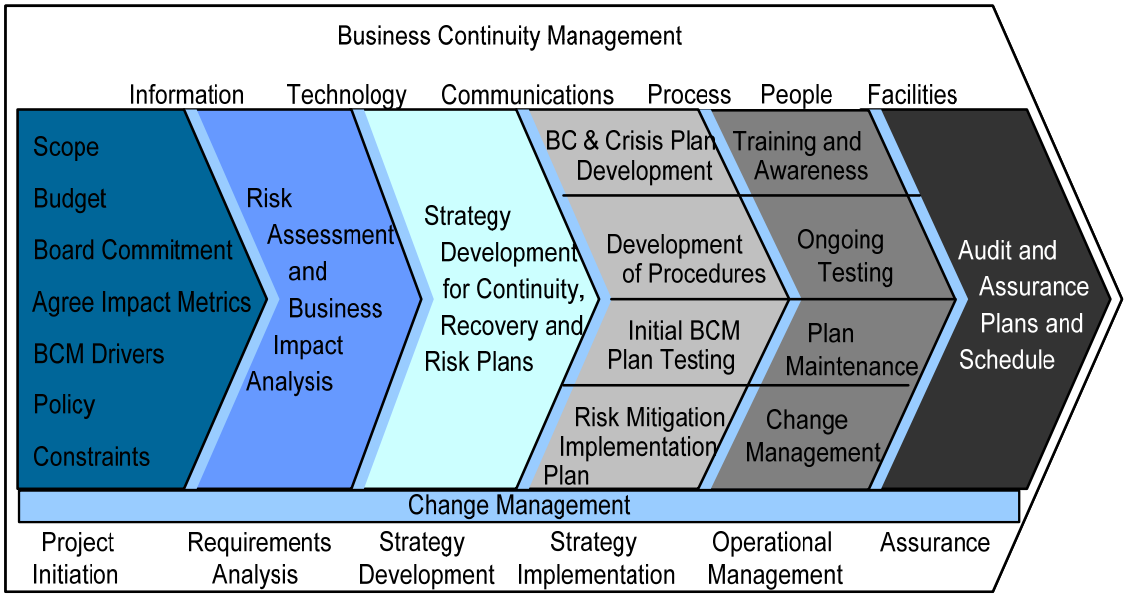

Figure 28: Organisation D's Business Continuity Management Framework

Organisation D's business continuity management framework consists of six sections namely the project initiation, requirements analysis, strategy development, strategy implementation, operational management and assurance. The most important elements of the project initiation section is about defining the scope and budget, obtaining client buy-in and agreeing on the constraints of the project. The next section is about conducting a requirement analysis by means of a risk assessment and business impact analysis. Once completed, the development of a business continuity management strategy must follow. The next section is dedicated to the implementation of these strategies. This includes the development of a business continuity management, crisis management and risk mitigation implementation plan together with the testing of each of these plans. The second last section is about operational management and consists of employee training, awareness and the maintenance of each plan. The final section is dedicated to the ongoing auditing of all the business continuity

management activities. Each of these sections should continuously be updated through the organisation's change management process.

An analysis of each of the frameworks implemented by the different organisations yields no shortcomings of the detailed objectives of business continuity management as derived from the content analysis. The subsequent chapter combines these detailed objectives with the frameworks proposed by the different organisation to develop a business continuity management framework.

7.4 CONCLUSION

The empirical study of this research is based on interviews with different participants who have expertise in the area of business continuity management and IT governance. These interviews focused on the objectives, evolution, relationship and level of integration between business continuity management and IT governance. The role players, main challenge and detailed objectives of business continuity management were discussed in depth with each participant. The interpretation of the results obtained from the empirical study is mostly consistent with the conclusions derived from the literature survey and content analysis. Based on these results, a business continuity management framework can be formulated. This framework is presented in the next chapter.

CHAPTER 8
A FRAMEWORK FOR BUSINESS CONTINUITY MANAGEMENT

8.1 INTRODUCTION

In chapter eight, a framework for business continuity management is proposed. The business continuity management framework is developed through the perspective of IT governance and is based on the results of the literature survey, content analysis and empirical study. In order to do so, background on the types of business continuity management disruptions is presented. The principle of business continuity management in a typical organisational environment is also discussed. The foremost challenge faced by management of business continuity is also discussed in this chapter. The chapter concludes by allocating the responsibilities of each of the business continuity management detailed objectives to the identified role players.

In this chapter, the main research question is answered:

- How does a framework for business continuity management look like when it is based upon a sound theoretical basis?

8.2 TYPES OF BUSINESS CONTINUITY MANAGEMENT DISRUPTIONS

There are various environmental factors that could potentially influence an organisation negatively. In previous chapters these factors were recognised as a risk, threat or event. As mentioned by Hiles & Barnes (2001:10), these factors can also be categorised under the following points:

- Acts of god: This includes all environmental events which man has no control over. Examples include tsunamis, floods, hurricanes and earth quakes;

- External, unintentional and intentional man–made events: Unintentional events include power failures, fires, etc. Intentional events are deliberately executed by man like terrorist attacks and security intrusions.; and

- Internal, unintentional and intentional man-made events: Unintentional events include accidental actions that have a negative influence on the organisation like power failures, hardware failures, data loss, etc. Intentional events are the malicious events executed by man to deliberately cause damage in the organisation like labour disputes, vandalism, data deletion, etc.;

The type of organisational disruption caused by these factors can be divided into three categories (Jones, 2005:44):

- Asset: This category focuses on assets of an organisation's environment. This not only covers organisational infrastructure including property, servers, networks, etc. but also other aspects like investments. This category is the easiest to measure as each asset has a financial value;

- Availability: Even though an asset might be in full working order, the usage of the asset can become disrupted. Examples are power failures, server downtime, the inaccessibility of organisational funds and denial of access whether it is physical (building security) or virtual (information systems). This category is more complex to measure when compared to the previous category. The financial losses associated with server downtime can be projected based on the historical information of similar disruptions; and

- Employee related: The last category is undoubtedly the most complex to measure as it is extremely difficult to measure and even more challenging to attach a financial value to it. Often, the two main aspects identified in this category are employee knowledge and skills.

Knowledge, in this particular instance, is the extent to which employees understand how the organisation operates (the logic behind the business) and is usually associated with experience. Skills are the ability of employees to perform their daily operations (conducting the business).

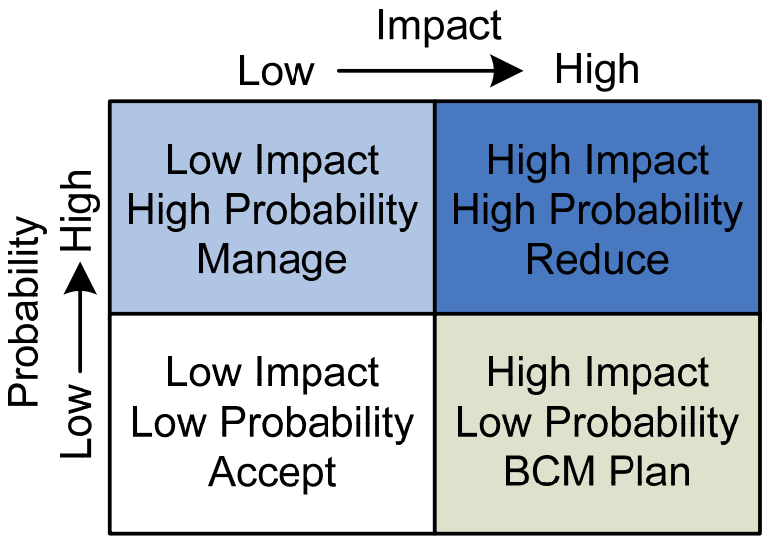

Figure 29: Factor Analysis Quadrants – Adopted from Hiles & Barnes (2001:136)

When analysing or prioritising factors that influence business continuity, the diagram presented in Figure 29 can be useful. Hiles & Barnes (2001:22) support the use of the factor analysis quadrant diagram and motivates that it is often more valuable to categorise factors according to their impact than type. To do so, each environmental factor is firstly assigned to the category of risk, threat or event, followed by the allocation of a specific block in the factor analysis quadrants. Each quadrant represents the severity of the impact that the factor has on the organisation together with the estimated materialisation probability of the factor. The insignificant factors are categorised in the bottom left quadrant and should be accepted by organisation without much concern. Alternatively, factors with a high probability but low impact should be managed accurately. An organisation's business continuity management plan should typically cover the factors listed in the bottom right quadrant where the disruption has a high impact but low probability. The factors assigned to the top right quadrant are of utmost importance to an organisation. This quadrant lists factors that can potentially have a major impact on the organisation and

that have a high probability of occurring. Organisations should prevent these factors from occurring. As Jones (2005:44) points out, history often repeats itself and therefore it is sensible to look at an organisation's critical historical losses when identifying the factors associated to this quadrant.

8.3 THE PRINCIPLE OF BUSINESS CONTINUITY MANAGEMENT

In order to develop a framework for business continuity management, the principle of business continuity management must first be explored. The principle of business continuity management positions the concept of business continuity in a typical organisation.

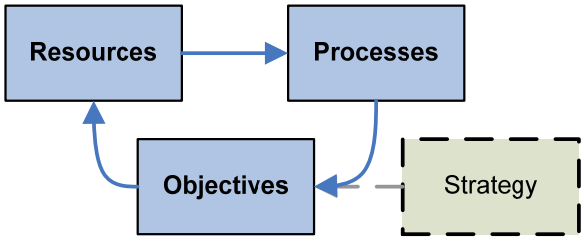

Figure 30: High Level Business Components – Adopted from The IT Governance Institute (2005:11)

Figure 30 details the typical high-level areas in an organisation that serves as a basis for the principle of business continuity management. The business areas of an organisation consist of resources, processes and objectives that are utilised according to the strategy of an organisation. Business processes utilise these resources to deliver, for instance, services or products to clients. Each business process should be aligned with the objectives of the organisation, whether it be profitable or on non profitable. An organisation's objectives should be aligned with the defined strategy. The objectives of an organisation direct the resources available to the organisation, from where the process follows an iterative cycle.

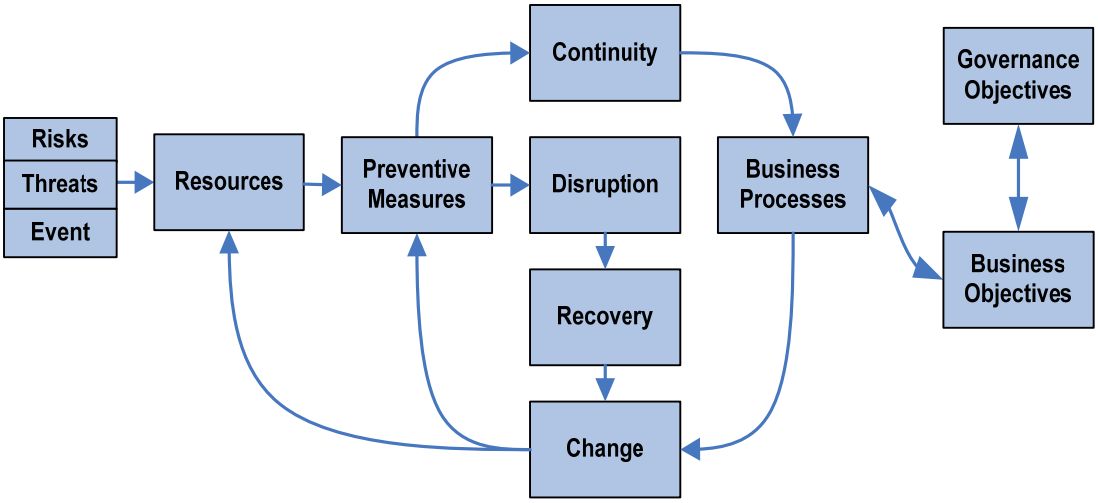

Figure 31: The Principle of Business Continuity Management

The principle of business continuity management is presented in Figure 31. An organisation's continuity can be disrupted by a risk, threat or event, as presented in previous chapters. Such a disaster will impact the continuity of the organisation's resources and might cause selected business processes to fail. In the case of a disruption of type risk, the organisation's preventive measures will attempt to void the impact of the disruption. The unforeseen nature of a threat or event might disrupt the continuity of resources because an organisation will probably not have implemented sufficient preventive measures to withstand the disruption. Ideally, these disruptions should be minimised by the preventive measures defined for risks of similar characteristics. However, typically this is seldom the case. Should these disruptions be countered by the preventive measures, the resources will continue to support the business processes. In cases where the preventive measures have failed to void the impact of a disruption, the recovery process will begin. The recovery process will initiate a change process where the disruption details will be used to prevent or minimise the impact of future occurrences of the disruption. The change process can also be initiated as a result of the alteration of business processes. The change process will then modify either the organisation's resources or change the preventive measures associated with the resource. The ultimate goal is for the organisational resources to enable business processes as managed by the business objectives. The business objectives are defined to support the governance objectives of the organisation, as defined by the organisation's strategy. It is

thus reasonable to state that business continuity management has a close relationship with an organisation's strategy (Elliott *et al.*, 1999:43; Herbane *et al.*, 2004:435), which is typically part of corporate governance.

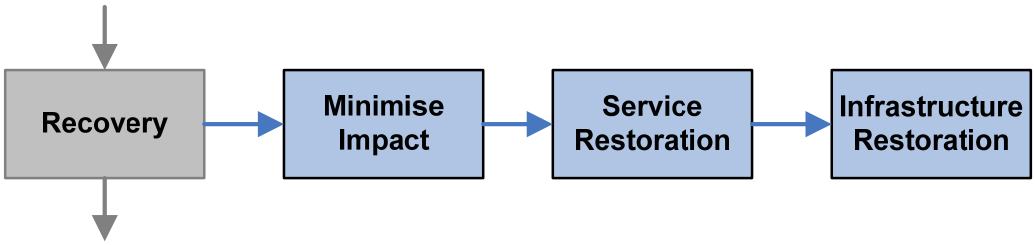

Figure 32: Business Continuity Management Recovery Principle

The principle of the business continuity management recovery component is detailed in Figure 32. The first objective is to minimise the impact of the disruption. The next objective is to restore the internal and external services as soon as possible. This will typically mean deliver services with temporarily solutions. Once service delivery can continue, the organisation can restore any temporarily solutions to the original state of the infrastructure.

8.4 A FRAMEWORK FOR BUSINESS CONTINUITY MANAGEMENT

The development of a business continuity management framework is based on the objective, detailed objectives and principle of business continuity management, as derived from the literature survey, content analysis and empirical study. The details of the objective and detailed objectives of business continuity management were presented in chapter six. The development of a business continuity management framework summarises these concepts at a high level.

Table 20 assigns an identifier to each detailed objective associated with the business continuity management framework. These identifiers are used as abbreviations in the remaining part of the research, where appropriate.

Table 20: Business Continuity Management Detailed Objectives ID's

Detailed Objective	ID
Resource Management	

Detailed Objective	ID
• Compliance	RE1
• Categorisation	RE2
• Identification, Allocation and Prioritising	RE3
• Monitoring and Reporting	RE4
Risk Management	
• Assessment	RM1
• Risk Reduction	RM2
• Business Impact Analysis	RM3
Business Continuity Management Guidelines	
• Policy	BG1
• Strategies	BG2
• Approaches	BG3
• Roles, Responsibilities and Tasks	BG4
• Monitoring and Reporting	BG5
Business Continuity Management Plan	
• Recovery Capability	BP1
• Alternative Processing	BP2
• Stand-by Arrangements	BP3
• Sub Plans	BP4
• Testing	BP5
• Communication and Distribution	BP6
• Awareness and Training	BP7
Post Resumption Review	
• Report Analysis	PR1

Detailed Objective	ID
• Update Business Continuity Management Plan	PR2
Change Management	
• Manage Change	CM1
Project Management	
• Methodology	PM1
• Project Plan	PM2
Auditing	
• Auditing	AU1

The business continuity management framework developed in this research is presented in Figure 33. Business continuity management is primarily focused on the availability of organisational resources. As the business processes are dependant on organisational resources, it is natural that the management of these resources is the foremost activity when ensuring business continuity management. Risk management controls the risks associated with the identified resources as well as the services supported by each resource. The result of risk management is an assessment, possible reduction and comprehensive analysis of each risk. The business continuity management guidelines aim to provide high-level instructions on the organisation's response to the identified risks. The business continuity management guidelines determine the approach and strategies of the organisation's business continuity management plan. The business continuity management plan is developed based on the business continuity management guidelines. This plan aims to document the detailed response activities planned by the organisation for each of the different risks. Once the recovery process of a disruption has been completed, an organisation needs to conduct a post resumption review to analyse whether and how the organisation recovered from the disruption. An important objective present in business continuity management is the management of changes in the organisation. An organisation's change management activities should synchronise business

continuity management with the actual environment of the organisation. Certain business continuity management detailed objectives can and should be implemented following a standard project management approach. Specifically, these objectives are resource management, risk management, the development of business continuity guidelines and the creation of a business continuity management plan. Throughout each of the objectives, the organisation should regularly conduct both internal and external audits. These audits ensure the quality of the organisation's business continuity management framework.

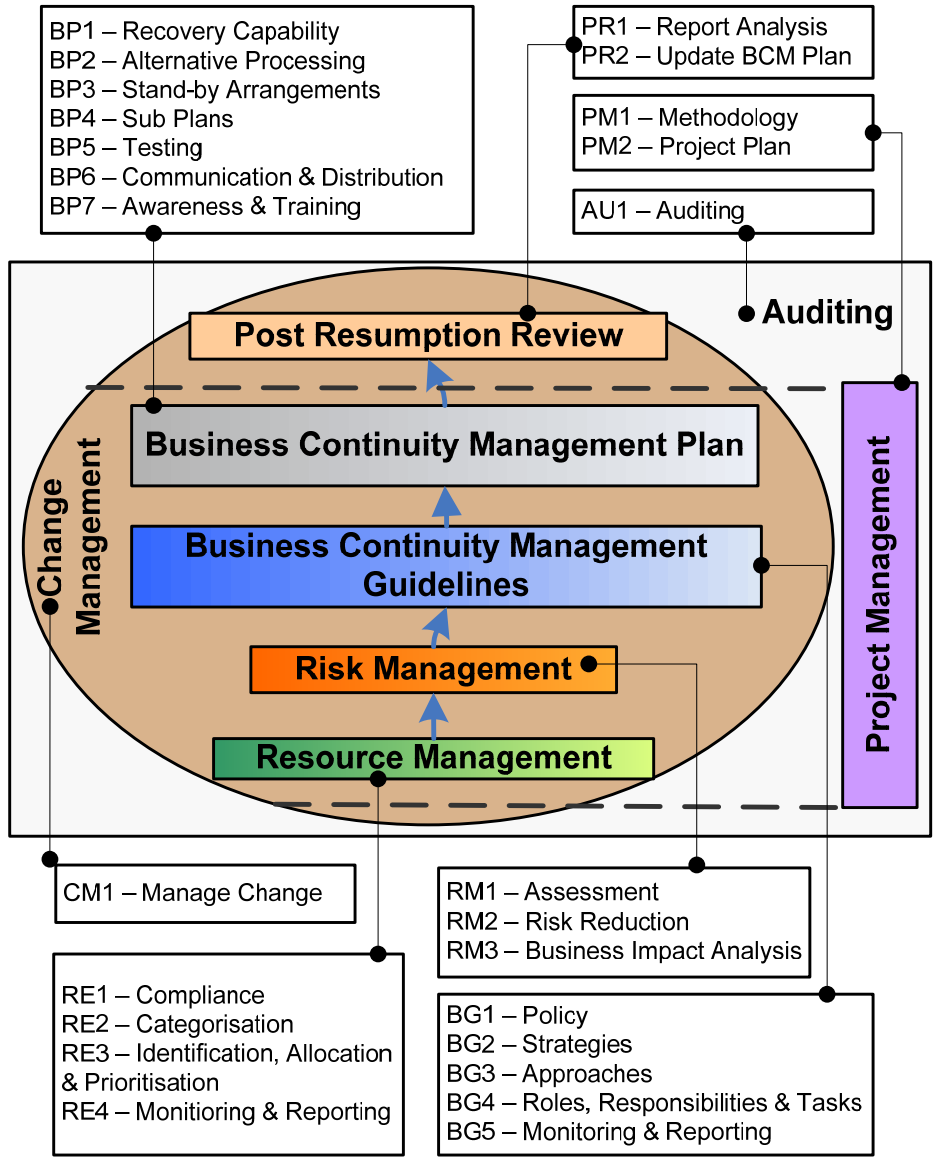

Figure 33: A Business Continuity Management Framework

8.5 THE RACI CHART

Based on the roles identified during the content analysis and empirical study, a RACI chart can be formulated. A RACI chart indicates whether a particular role player is responsible, accountable, consulted and / or informed about the detailed objective.

Table 21: Business Continuity Management RACI Chart

Detailed Objective	CEO	CIO	CFO	CRO	COO/Head of Operations	Head of Development	Chief Architect	BCM Board	PMO	BCM Committee	BCM Manager
RE1	I	C	C	C	C	C	C	A		A	R
RE2				A				A,I		R,A	R
RE3				A				A,I		R,A	R
RE4	I	I	I	A	I	I	I	A,I		R,A	R
RM1				A				A,I		R,A	R
RM2		C	C	A	C	C	C	A,I		R,A	R
RM3	C	C	C	A	C	C	C	A,I		R,A	R
BG1	I	C,I	C,I	A,C	C,I	C,I	C,I	A,I		R,A	R
BG2	I	C,I	C,I	A,C	C,I	C,I	C,I	A,I		R,A	R
BG3				A				A,I		R,A	R
BG4				A				A,I		R,A	R
BG5	I	I	I	A	I	I	I	A,I		R,A	R
BP1		C	C	A,C	C	C	C	A,I		R,A	R
BP2		C	C	A,C	C	C	C	A,I		R,A	R
BP3		C	C	A,C	C	C	C	A,I		R,A	R
BP4		C	C	A,C	C	C	C	A,I		R,A	R
BP5	I	I	I	A,I	I	I	I	A,I	I	R,A	R
BP6				A				A,I		R,A	R

Detailed Objective	CEO	CIO	CFO	CRO	COO/Head of Operations	Head of Development	Chief Architect	BCM Board	PMO	BCM Committee	BCM Manager
BP7				A				A,I		R,A	R
PR1	I	I	I	A,I	I	I	I	A,I		R,A	R
PR2				A				A,I		R,A	R
CM1					A			A,I	R	R,A	R
PM1								A,I	R,A	R,A	R
PM2								A,I	R,A	R,A	R
AU1	I	I	I	I	I	I		A,I	R,A	R,A	R

8.6 THE MAIN CHALLENGE OF BUSINESS CONTINUITY MANAGEMENT

The empirical study indicated various challenges faced by practitioners when practising business continuity management. Obtaining sufficient funding proved to be the most challenging part of business continuity management, according to this research.

The practitioners indicated that organisations find it difficult to motivate expenditures associated with business continuity management. As business continuity management does not always result in a return on investment, business continuity managers find it a challenging task to obtain the funding required to ensure business continuity. Cummings (2005:s4) states that from a financial perspective, business continuity management activities like disaster recovery management, is clearly an expense, but by integrating it with business objectives, more value can be derived from the costs. Thomas & Preston (2005:34) explain that an organisation can reduce some of the costs and efforts associated with business continuity management by taking out insurance. However, Hiles & Barnes (2001: 357) warn that organisations do not migrate all their risks and responsibilities to the insurer by taking out insurance. There are still certain business continuity management activities

that need to be controlled by the organisation to ensure a seamless recovery through the interaction with the insurer. Graham & Kaye (2006:247) also point out that most organisations commit to 'of the self' insurance and warn that typically these packages are not designed according to the organisation's unique requirements. By committing to an insurance instalment, some of the risks of organisations can be migrated to an insurance company.

The following points are presented as motivation to why organisations should commit to the costs associated with business continuity management:

- Marketing (Hiles & Barnes, 2001:363). An organisation could typically spend three times the amount of its annual marketing budget to keep and regain its market share after a serious disruption. A portion of this amount could be spend on business continuity management;

- Financial (Hiles & Barnes, 2001:363). Different financial motivations can be connected to business continuity management expenditures. For instance, in some cases an organisation might be unable to deliver service levels (as a result of a disruption) and as a result certain penalty fees are payable to clients. A worse case would be if an organisation loses its credit control information, resulting in the write-off of capital;

- Testing (Mitts, 2005:8). The testing of certain disruption scenarios can calculate the financial cost associated with disruption. In this way a portion of the business continuity management expenditures can be justified;

- Legislative requirements (Hiles & Barnes, 2001:363). Various legislations force organisations to implement business continuity management. If this is the case, organisations should not assign these expenditures to business continuity management but rather as part of their daily operational costs;

- Quality (Hiles & Barnes, 2001:363). Business continuity management contributes towards the delivery of quality services or products. In doing so, organisations will complement their quality accreditations (like ISO 9000) and are more likely to have successful audits. Two examples of the benefits derived from this are the decrease of production costs and the increase in market share; and

- Value preservation (Herbane, 2004:435). The ability for organisations to quickly recover from disruptions with minimal impact and loss assists them in continuing the execution of the organisational strategy and therefore materialising their competitive advantage. Business continuity management therefore contributes towards the sustainability of an organisation's strategy by means of value preservation.

Doughty (2002) argues that even though business continuity management expenditures should ideally be seen as an investment, it is hardly ever the case. Organisations have various options on how to commit to the costs associated with business continuity management. Some of these funding options are proposed by Doughty (2002):

- Corporate funding where expenditures related to business continuity management should be budgeted and allocated from a corporate level. Organisations should see this as part of their operating expenditures (Cummings:s4) and social responsibility. In the case of an threat or event materialising, evidence of the organisation's commitment to prevent such incidents, exists;

- Business unit funding is when each business unit in the organisation funds business continuity management. The advantage to this is that each business unit knows what is important to the continuity of their operations, whereas the disadvantage is that the expenditures can easily be prevented should the unit's budget be limited; and

- IT funding is when the organisation's IT department has the responsibility of ensuring business continuity. As discussed previously, the traditional focus of business continuity management mainly focussed on IT, in which case this funding option would have been adequate. However, in the research findings it was highlighted that business continuity management has evolved to mainly focus on business processes and only utilise IT as a business enabler (Elliott *et al*., 1999:43). For this reason, IT funding is disqualified as an adequate motivation for funding business continuity management expenditures.

Practitioners have identified funding as the most challenging part of business continuity management. However, this section presents various motivations for organisations to commit to these expenses, as well as different funding options.

8.7 CONCLUSION

The main objective of this chapter was to present a business continuity management framework, as derived from the literature survey, content analysis and empirical study. The typical high-level components of an organisation, which consists of the relationship between resources, processes and objectives, were presented as a background to the framework. Based on these high-level business components, the principle of business continuity management was described. A RACI chart was also developed that mapped each of the key role players of business continuity management against the detailed objectives of the business continuity management framework.

Chapter nine is the concluding chapter of this research. The chapter illustrates the apparent paradigm shift in the area of business continuity management. The chapter also presents a summary of the developed business continuity management framework and discuss the main challenges experienced when implementing such a framework. In conclusion, some recommendations and future research areas are presented.

CHAPTER 9
CONCLUSIONS, RECOMMENDATIONS AND FUTURE RESEARCH

9.1 INTRODUCTION

The conclusions of the research are presented in the final chapter. The research consists of a literature survey, content analysis and empirical study and is aimed at developing a business continuity management framework. In this chapter, an overview of the business continuity management framework developed in this research is summarised. The evolution of business continuity management has resulted in an evident paradigm shift, which is discussed in this chapter. In conclusion, a few recommendations and future research topics based is also presented.

9.2 IT GOVERNANCE AND BUSINESS CONTINUITY MANAGEMENT

This research leverages of the theory of IT governance and specifically the COBIT and ITIL IT governance frameworks. Based on this, a framework for business continuity management is developed.

The objective of IT governance is defined as a framework of IT-related processes which is aligned with business strategy and focused on the delivery of maximum IT value from disciplined IT investments, while balancing risks. The COBIT and ITIL IT governance frameworks have processes dedicated to manage the continuity of an organisation, specifically DS4 (ensure continuous service) and ITSCM (IT service continuity management) respectively. The manner in which these processes conceptualise business continuity management were analysed using the content analysis.

The business continuity management framework developed in this research can be integrated with COBIT and ITIL. The PO2 (define the information architecture), PO9 (assess and manage risks), AI2 (acquire and maintain

application software), AI4 (enable operation and use) and DS1 (define and manage service levels) COBIT control objectives serve as inputs to the frameworks, whereas the outputs are PO2, DS1, DS2 (manage third party services), DS8 (manage service desk incidents), DS9 (manage the configuration), DS11 (manage data), DS13 (manage operations) and ME1 (monitor and evaluate IT performance). The ITIL process elements that are inputs to the framework are Service Level Management, Availability Management, Incident Management, Problem Management and Service Desk. The outputs of the framework relate to ITIL's Service Level Management, Capacity Management, Configuration Management and Change Management.

The relationship between IT governance and business continuity management is identified in this research. Risk management and IT governance are two components of corporate governance. One component of risk management is business continuity management which consists of, amongst others, disaster recovery. Disaster recovery aims to ensure the IT continuity of an organisation and has a direct relationship with IT governance. The concept of disaster recovery came to be during the evolution of business continuity management, as discussed in the next section.

9.3 THE PARADIGM SHIFT OF BUSINESS CONTINUITY MANAGEMENT

The result of the research clearly identifies a paradigm shift in the area of business continuity management. This paradigm shift is a result of the evolution of business continuity management as identified through the literature survey and empirical study.

Traditionally, business continuity management focused mainly on continuity issues regarding an organisation's IT infrastructure. This was as a result of the organisation's fundamental dependency on IT. Consequently, the continuity of most organisations was traditionally seen as the responsibility of the IT department (Graham & Kaye, 2006:15). However, over the past couple of years many business disruptions and disasters made executives realise

that this traditional scope is not adequate to ensure the overall continuity of their organisation. Specifically, Elliott *et al.* (1999:43) mention that both practitioners and academics have ignored the human related aspects. In addition, government institutions have identified specific measures that are compulsory to be implemented by organisations and these measures have consequently been included in legislations and regulations. This resulted in the establishment of various other subcomponents focussing on the continuity of specific areas in organisations. The most prominent of these subcomponents is disaster recovery. As discussed in previous chapters, disaster recovery is dedicated to the continuity of an organisation's IT infrastructure.

The evolution of business continuity management has increased its traditional scope of IT to place more emphasis on the business operations of an organisation. As a result, the responsibility of business continuity management has shifted from the IT department to include the business departments. This paradigm shift is referred to by Hiles & Barnes (2001: 290) as corporate continuance management. Elliott *et al.* (1999:43) explain that this shift forces a culture change in organisations, as the role of business continuity management have become more strategic oriented to ensure a competitive advantage. Herbane *et al.* (2004:435) also support the suggestion that business continuity management has evolved from an IT focused essential to a strategic advantage and obligation.

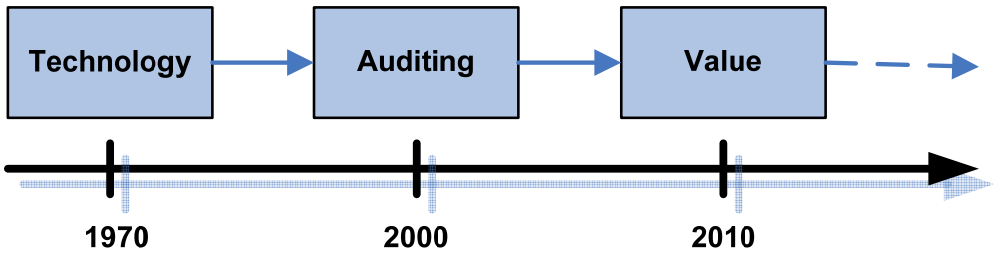

Figure 34: Paradigm Shift of Business Continuity Management (Adopted from Swartz *et al.* (2003:69))

The paradigm shift of business continuity management has also been recognised by Swartz *et al.* (2003:69), as illustrated by Figure 34. Initially, business continuity management had a strong focus on technology,

specifically large corporate information systems. The focus then shifted to the auditing of both corporate and office systems, as dictated by regulatory and legislative requirements. The present focus of business continuity management is moving towards the delivery of strategic value to the organisation.

Many executives have realised the importance of business continuity management or have been tasked to implement specific elements of business continuity management. Often, these executives do not have the necessary skills or experience to implement business continuity management. Consequently, many practitioners have obtained different qualifications and certifications to demonstrate their professionalism as business continuity management specialists. This is proven by the exponential increase of certifications issued by the Business Continuity Institute and the Disaster Recovery Institute International (Hiles & Barnes, 2001: 291). In cases where organisations do not have the necessary business continuity management skills, or where the scope of business continuity management is beyond the capacity of individuals, organisations often acquire the services of industry experts in the form of consultants. This resulted in the offering of 'one-stop shops' where consulting firms offer generic business continuity management frameworks, causing the business continuity market to grow globally at 25% for developed countries (Hiles & Barnes, 2001: 291). In the researcher's opinion, the lack of easily accessible business continuity management frameworks (like the one proposed in this research) has contributed to the need of these third party services.

9.4 BUSINESS CONTINUITY MANAGEMENT FRAMEWORK SUMMARY

The main objective of this research is to take the initial steps towards the development of a business continuity management framework. In order to achieve this goal, a specific research approach has been followed which includes a literature survey, content analysis on the two most popular IT governance frameworks (namely COBIT and ITIL) and an empirical study where six experts representing four organisations were interviewed. A

summary of the business continuity management framework developed is presented in Figure 35.

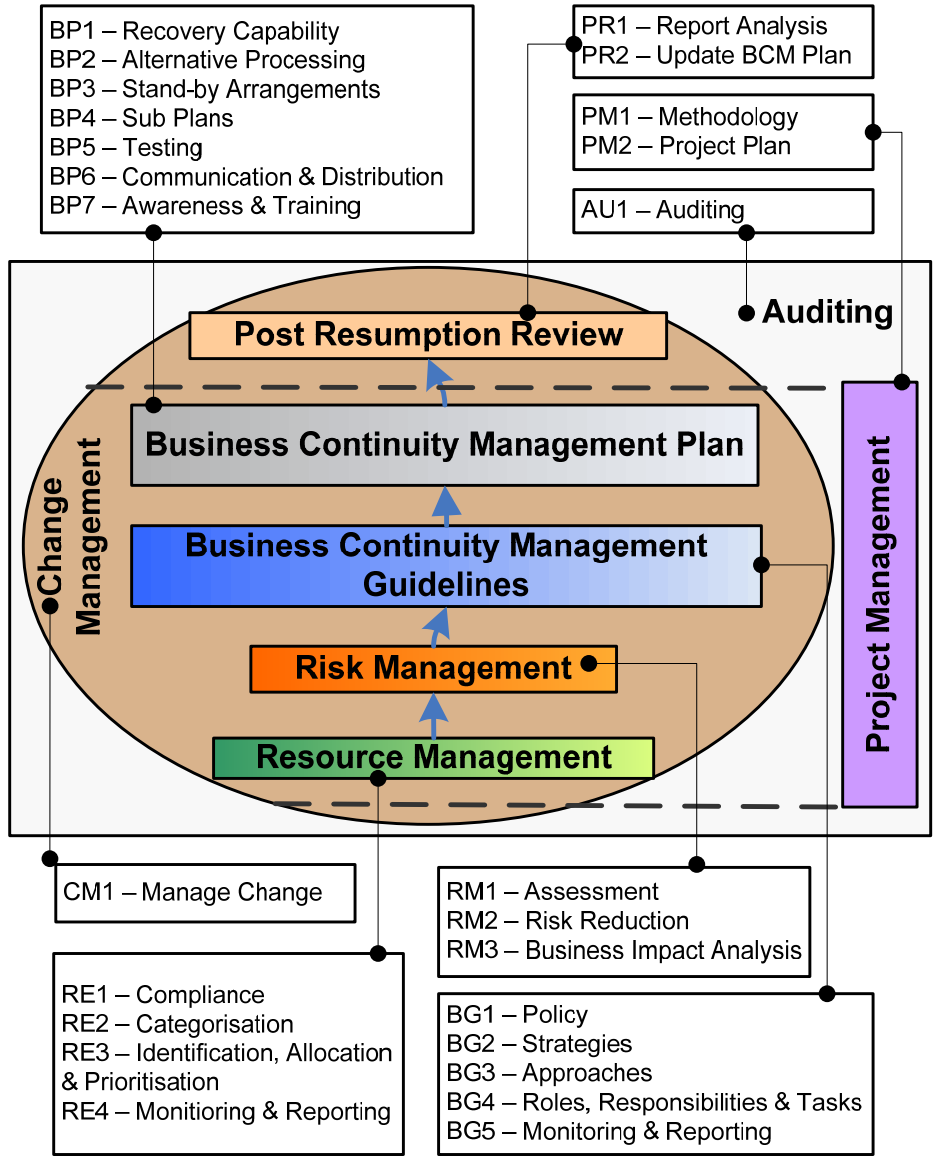

Figure 35: Business Continuity Management Framework Summary

The objective of business continuity management, as defined in chapter six, is to sustain the continuity of an organisation by analysing risks, threats and events, as well as the impact it might have on an organisation and then to design preventive and response plans. The detailed objectives of business continuity management were also discussed in chapter six and consist of resource management, risk management, the development of business continuity management guidelines, the development of a business continuity

management plan, post resumption review, project management, change management and auditing.

9.5 RECOMMENDATIONS

The paradigm shift of business continuity management explains how it evolved from an IT initiative to a business responsibility. The continuity of an organisation is dependant on much more than just the IT infrastructure of an organisation. Comprehensive business continuity management now consists of a variety of subcomponents like planning for disaster recovery, crisis management, emergency response and public relations. As a result of this increased scope, academics and practitioners must therefore realise that the accountability of business continuity management lies within each department of the organisation. Particular components of business continuity management should still be dedicated to specific departments and executives e.g. disaster recovery planning should always remain the responsibility of the IT department and ultimately the CIO. A governing body consisting of various executives like the CEO, CIO, CFO, CRO and COO must oversee and integrate the implementation of these components. The researcher therefore recommends that organisations recognise business continuity management as the enterprise implementation of preventive and responsive measures with the goal of ensuring the availability of the entire organisation, despite the materialisation of an interruption. In addition, the research also supports the prediction made by Graham & Kaye (2006:7) who expect the International Standards Organisation (ISO) to soon publish an enterprise risk management standard. The quality of business continuity management frameworks should improve significantly should such a standard be published.

9.6 FUTURE RESEARCH

The initial steps towards the development of a formal business continuity management framework are presented in this chapter. Based on this research, the following future research areas can be explored:

- An expansion of the business continuity management framework proposed in this research. This also includes, amongst others, the development of management guidelines (e.g. the goals and metrics of each detailed objective) and maturity models which organisations can use to measure the state of their business continuity management framework implementation;

- A case study that consists of the practical implementation of the proposed business continuity management framework. Such research will enhance the comprehensiveness of the framework and possibly highlight shortcomings of and improvements to the framework;

- An exploration to identify whether COBIT's control objective and ITIL's process elements, namely DS4 and ITSCM respectively, is sufficient to ensure efficient and effective disaster recovery which is one subcomponent of business continuity management. A critical component of this research would be the completion of an intensive empirical study with organisations that have experienced business disruptions. A prerequisite would be for these organisations to have successfully implemented COBIT and/or ITIL;

- The development of a cost-benefit model which can guide practitioners on prioritising business continuity management implementations while ensuring maximum return on investment; and

- A research study investigating the quantitative nature of the business continuity management framework proposed in this research, or the COBIT and ITIL IT governance frameworks.

9.7 CONCLUSION

Business continuity management and IT governance are topics that have received vast attention and transformation in the past couple of years. To a certain degree, IT governance has evolved to develop generic predefined

practitioner oriented frameworks that are fairly easily accessible and internationally acceptable. Unlike IT governance, business continuity management has not yet matured to such a degree.

To objective of this research is to leverage of the success of IT governance to develop a theoretical basis for business continuity management from which a business continuity management framework can be developed. Specifically, the COBIT and ITIL IT governance frameworks were examined by means of a research method called content analysis. To complement this method, the research methodology included a literature survey and empirical study. The results obtained from each activity were interpreted according to the interpretivism paradigm. The conclusions of the research established a theoretical basis for business continuity management from which a framework was developed.

The business continuity management framework proposed in this research is aimed at practitioners who want to ensure the continuous delivery of business critical operations by means of preventive and responsive plans, despite the materialisation of a business disruption. The business continuity management framework developed covers eight key areas in an organisation and consists of 26 detailed objectives. The sequential order in which each detailed objective should be executed, together with the relationship between them, were addressed in this research.

This research confirmed the necessity for a paradigm shift in the area of business continuity management. Traditionally, the IT department in an organisation was accountable for business continuity management as a result of the strong focus that the continuity of an organisation had on IT. An increasing number of organisations have now reconsidered the scope of business continuity management to place more emphasis on ‘the rest of the business’. This has resulted in the responsibility of business continuity management to be migrated from the IT department to the different business departments. The business departments should be complemented with a governing body dedicated to the regulation of the different implementations.

Unfortunately, organisations now find the funding of these initiatives very challenging as it is seen as an expenditure and not an investment. In a response to this challenge, various motivations why organisations should practise business continuity management together with different approaches to motivate the related expenditures were discussed. The research also illustrated proof that business continuity management has a strong relationship with an organisation's strategy and therefore emerging to become a competitive advantage because of its value preservation characteristics.

In conclusion, a quote from Graham & Kaye (2006:193) illustrates the researcher's opinion about the necessity of business continuity management:

'Some things are best left to change – a card game or roll of the dice. Other things need to be planned, carefully planned and tested.'

GLOSSARY

AMDB – Availability management database

BCM – Business continuity management

BI – Business intelligence

CDB – Capacity management database

CEO – Chief executive officer

CIO – Chief information officer

CMDB – Configuration management database

COBIT – Control objectives for information and related technology

COO – Chief of operations

CPU – Central processing unit

CRM – Customer relationship management

CRO – Chief risk officer

DS – Delivery and support

ERP – Enterprise resource planning

ETO – Resumption time objective

HIPAA – Health insurance portability and accountability act

ICT – Information and communication technology

IS – Information systems

ISACA – Information systems and control association

ISO – International standards organisation

IT – Information technology

ITIL – IT infrastructure library

ITSCM – IT service continuity management

KWIC – Keywords in context

MTO – Maximum tolerable outage

OLA – Operational level agreement

OLR – Operational level requirement

PMBOK – Project management body of knowledge

PMO – Project management office

RACI – Responsible, accountable, consulted and/or informed

RAD – Rapid application development

RDO – Recovery data objective

RFC – Request for change

RPO – Recovery point objective

RTO – Recovery time objective

SCM – Supply chain management

SLA – Service level agreement

SLM – Service level management

SLR – Service level requirement

REFERENCES

ANTHES, G.H. 2004. Model mania. Computer World (US), March 2004, vol.38, no.10, p.41 – 44.

BAKSHI, S. & RAFEQ, A. 2005. "The Asian tsunami: a wake-up call for traditional disaster recovery planning". [Online]. Available: http://www.isaca.org/Template.cfm?Section=Security&CONTENTID=19766&TEMPLATE=/MembersOnly.cfm [Cited December, 2005].

BANDAROUK, T.V. & RUEL, H.J.M. 2004. Discourse analysis: making complex methodology simple. Proceedings of the 12th European Conference in Information Systems.

BEASLEY, M.S., CLUNE, R. & HERMANSON, D.R. 2005. "Enterprise risk management: An empirical analysis of the factors associated with the extent of implementation". Journal of Accounting and Public Policy, November 2005.

BENSTON, G.J. & HARTGRAVES, A.L. 2002. Enron: what happened and what we can learn from it. Journal of Accounting and Public Policy, May 2002, vol.21, no.2, p.105 – 127.

BURN, M.J. & SZETO, C. 1999. A comparison of the views of business and IT management on the success factors for strategic alignment. Information and Management, September 1999, vol.37, no.4, p.197 – 216.

CALDERON, T.G. 2003. Assurance and recovery cost optimization in business continuity planning. Internal Auditing, March / April 2003, vol.18, no.2, p.20 – 30.

CALDERON, T.G. & DISHOVSKA, M. 2005. Transitioning from disaster recovery management to business continuity management. Internal Auditing, March / April 2005, vol.20, no.2, p.21 – 29.

CARLEY, K. 1993. Coding choices for textual analysis: a comparison of content analysis and map analysis. Sociological Methodology, 1993, vol.23, p.75 – 126.

CARROLL, P., RIDLEY, G. & YOUNG, J. 2004. COBIT and its utilisation: a framework from the literature. System Sciences, January 2004, p.233 – 240.

COX, J. 2004. Implementing ITIL. Network World, October 2004, vol.21, no.40, p.60 – 61.

CUMMINGS, J. 2005. The new business continuity. Network World, May 2005, vol.22, no.20, p.s3 – s4.

DAHLBERG, T. & KIVIJARVI, H. 2006. An integrated framework for IT governance and the development and validation of an assessment instrument. Proceedings of the 39th Annual Hawaii International Conference on System Sciences, January 2006, vol.8, p.194b – 194b.

DAMIANIDES, M. 2005. Sarbanes-Oxley and IT governance: new guide on IT control and compliance. Information Systems Management, April 2005, vol.22, no.1, p.77 – 86.

DOUGHTY, K. 1999. Selecting the “right” business continuity planning recovery strategy. [Online]. Available: http://www.isaca.org/Content/ContentGroups/InfoBytes/19991/Selecting_the_Right_Business_Continuity_Planning_Recovery_Strategy.htm [Cited October, 2005].

DOUGHTY, K. 2002. Business continuity: A business survival strategy. [Online]. Available: http://www.isaca.org/Content/ContentGroups/Member_Content/Journal1/20023/Business_Continuity_A_Business_Survival_Strategy.htm [Cited September, 2005].

DUBE, D. 2004. American ITIL: best practices win converts. Network World, August 2004, vol.21, no.35, p.1 – 2.

ELLIOTT, D., SWARTZ, E. & HERBANE, B. 1999. Just waiting for the next bang: business continuity planning in the UK finance sector. Journal of Applied Management Studies, June 1999, vol.8, no.1, p.43 – 61.

EXLER, R. 2003. "IT governance frameworks." [Online]. Available: http://www2.cio.com/analyst/report1559.html [Cited June 2005].

GAYNOR, D. 2002. IT governance. Accountancy Ireland, August 2002, vol.34, no.4, p.28.

GRAHAM, J. & KAYE, D. 2006. A risk management approach to business continuity. Brookfield, Connecticut USA: Rothstein Associates Inc.

HERBANE, B., ELLIOTT, E. & SWARTZ, E.M. 2004. Business continuity management: time for a strategic role? Long Range Planning, October 2004, vol.37, no.5, p.435 – 457.

HILES, A. & BARNES P. 2001. The definitive handbook of business continuity management. Chichester, UK: John Wiley and Sons Ltd.

HOCHSTEIN, A., ZARNEKOW, R. & BRENNER, W. 2005. ITIL as a common practice reference model for IT service management: formal assessment and implications for practice. The 2005 IEEE International Conference on e-technology, e-commerce and e-service. March / April 2005, p.704 – 710.

HOFFMAN, T. 2003. Disparate views of IT governance spark debate. Computer World (US), May 2003, vol.37, no.18, p.14.

HOFFMAN, T. 2004. IT governance is on the hot seat. Computer World (US), July 2004, vol.38, no.28, p.6.

HWANG, J.D. 2002. Information resources management: new era, new rules. IT Professional, November/December 2002, vol.4, no.6, p.9 – 18.

HWANG, J.D. & LIU, S. 2003. Challenges to transforming IT in the US government. IT Professional, May/June 2003, vol.5, no.3, p.10 – 15.

IT GOVERNANCE INSTITUTE. 2000. "COBIT 3rd edition executive summary." [Online]. Available: http://www.isaca.org/execsum.pdf [Cited June, 2005].

IT GOVERNANCE INSTITUTE. 2005. Cobit 4.0 [Online]. Available: http://www.isaca.org/AMTemplate.cfm?Section=Overview&Template=/ContentManagement/ContentDisplay.cfm&ContentID=22940 [Cited March, 2005].

JONES, M. 2005. Bettering the odds with risk management. American Agent & Broker, October 2005, vol.77, no.10, p.44 – 45.

KAN, A.R. 2003. Managing a multi-billion dollar IT budget. Software Maintenance, September 2003, p.2.

KIM, G. 2003. Sarbanes-Oxley, fraud prevention, and IMCA: a framework for effective controls assurance. Computer Fraud & Security, September 2003, vol.2003, no.9, p.12 – 16.

KOCH, C. 2002. "The powers that should be – governance." [Online]. Available: http://www.cio.com/archive/091502/powers.html?printversion=yes [Cited March, 2005].

KRACAUER, S. 1953. The challenge of qualitative content analysis. The public opinion quarterly, 1953, vol.16, no.4, p.631 – 642.

KRIPPENDORFF, K. 2004. Content Analysis: an introduction to its methodology, 2nd ed. London, UK: Sage Publications.

LAM, W. 2002. Ensuring business continuity. IT Professional, May / June 2002, vol.4, no.3, p.19 – 25.

MANNING, B.R.M. 1999. Year 2000 and all that: securing business continuity. Engineering Science and Education Journal, December 1999, vol.8, no.6, p.243 – 248.

McCARTHY, D. & PUFFER, S. 2002. Corporate governance in Russia: towards a European, US or Russian model? European Management Journal, December 2002, vol.20, no.6, p.630 – 640.

MENA, C. 2002. Making security a team effort. Optimize, October 2002, p.38 – 43.

MITTS, J.S. 2005. Business continuity and disaster recovery plans: how and when to test them. EDPACS, November 2005, vol.33, no.5, p.8 – 24.

MORENCY, J. 2005. Best practice, practice, practice. Network World. January 2005, vol.22, no.1, p.37.

MUSAJI, Y.K. 2002. "Disaster recovery and business continuity planning: testing an organisation's plans." [Online]. Available: http://www.isaca.org/Content/ContentGroups/Member_Content/Journal1/20023/Disaster_Recovery_and_Business_Continuity_Planning_Testing_an_Organisations_Plans.htm [Cited Augustus, 2005].

NELSON, J. 2005. Corporate governance practices, CEO characteristics and firm performance. Journal of Corporate Finance, March 2005, vol.11, no.1 – 2, p.197 – 228.

NEUENDORF, K.A. 2002. The content analysis guidebook. London, UK: Sage Publications.

OFFICE OF GOVERNMENT COMMERCE. 2002a. Service Management. London: The Stationery Office.

OFFICE OF GOVERNMENT COMMERCE. 2002b. Service Delivery. London: The Stationery Office.

OFFICE OF GOVERNMENT COMMERCE. 2002c. Service Support. London: The Stationery Office.

PARKER, M.M., PETERSON, R.R. & RIBBERS, P.M.A. 2002. Designing information technology governance processes: diagnosing contemporary practices and competing theories. System Sciences, January 2002, p.3143 – 3154.

PATEL, N.V. 2002. Global e-business IT governance: radical re-directions. System Sciences, January 2002, p.3163 – 3172.

PRICE, E.S. 2004. The new scope of business continuity. AIIM E – Doc Magazine, July / August 2004, vol.18, no.4, p.34 – 36.

ROBERTS, C.W. 1989. Other than counting words: a linguistic approach to content analysis. Social Forces, September 1989, vol.68, no.1, p.147 – 177.

RODRIGUEZ, H & MARKS, D. 2006. Disasters, vulnerabilities and government response: where (how) have we gone so wrong? Corporate Finance Review, May / June 2006, vol.10, no.6, p.5 – 13.

RUTHERFORD, J., RILEY, J. & BOYER, L. 2002. Business as usual with standby systems, services and solutions. ABA Bank Compliance, January / February 2002, vol.23, no.1, p.4 – 11.

SAYANA, S.A. 2005. Auditing business continuity. [Online]. Available: http://www.isaca.org/Content/NavigationMenu/Students_and_Educators/ IT_Audit_Basics/ Auditing_Business_Continuity.htm [Cited December, 2005].

SCHULTZ, E. 2005. Aligning disaster recovery and security incident response. Computers & Security, October 2005, vol.24, no.7, p.505 – 506.

SCHWARZ, A & HIRSCHHEIM, R. 2003. An extended platform logic perspective of IT governance: managing perceptions and activations of IT. Journal of Strategic Information Systems, 2003, vol.12, no.12, p.129 – 166.

SHEFFI, Y. 2005. The resilient enterprise: overcoming vulnerability for competitive advantage. London: The MIT Press.

SOBEL, P.J. & REDING, K.F. 2004. Aligning corporate governance with enterprise risk management. Management Accounting Quarterly, 2004, vol.5, no.2, p.29.

SOHAL, A.S. & FITZPATRICK, P. 2002. IT governance and management in large Australian organisations. International Journal of Production Economics, 2002, vol.75, no.1, p.97 – 112.

SWARTZ, E., ELLIOT, D. & HERBANE, B. 2003. Greater than the sum of its parts: business continuity management in the UK finance sector. Risk Management: An International Journal, January 2003, p.65 – 80.

THE BUSINESS CONTINUITY INSTITUTE. 2006. "Government of Saskatchewan Business Continuity Guide". [Online]. Available: http://www.thebci.org/businesscontinuityguides.htm [Cited June, 2006].

THOMAS, B.B. & PRESTON, L.W. 2005. Insuring business continuity. Strategic Finance, May 2005, vol.86, no.11, p.34 – 39.

YOUNG, K. 2000. "Continuity in a virtual world." [Online]. Available: http://www.isaca.org/Content/ContentGroups/InfoBytes/20001/Continuity_in_a_Virtual_World.htm [Cited Julie, 2005].

VAN GREMBERGEN, W. 2003. Introduction to the minitrack "IT governance and its mechanisms" HICSS 2003. System Sciences, January 2003, p.242.

WEILL, P & ROSS, J.W. 2003. IT governance: how top performers manage IT decisions rights for superior results. Boston: Harvard Business School Publishing.

WEILL, P. & ROSS, J.W 2004. "Recipe for good governance." [Online]. Available: http://www.cio.com/archive/061504/keynote.html [Cited April, 2004].

WORTHEN, B. 2005. ITIL power: why the IT Infrastructure Library is becoming the most popular process framework for running IT in America, and what it can do for you. CIO, September 2005, vol.18, no.22, p.1.