

A Cyclic Approach to Business Continuity Planning

This dissertation comprises work completed in the field of

INFORMATION TECHNOLOGY

and is submitted by

JACQUES BOTHA

in accordance with the requirements for the degree of

MAGISTER TECHNOLOGIAE : INFORMATION TECHNOLOGY

at the

PORT ELIZABETH TECHNIKON

Promoter : Prof. R. Von Solms

Year : 2002

With acknowledgement for valued assistance towards the finalisation of my dissertation:

To God, for creativity, strength and motivation.

To Prof Rossouw von Solms for guidance, encouragement and the sharing of a wealth of experience.

To the National Research Foundation and P.E. Technikon for financial support in the pursuance of my goals.

Contents

Chapter 1 Introduction.....	1
1.1 Background.....	1
1.2 Problem Statement	2
1.3 Objectives	3
1.4 Research Methodology.....	4
1.5 Structure of Dissertation.....	5
Chapter 2 Information Security: An Introduction	7
2.1 Introduction.....	7
2.2 Information Security	8
2.2.1 The importance of information security	8
2.2.2 The three pillars of information security	10
2.3 Business Continuity Planning (BCP)	11
2.3.1 Disasters and Business Continuity Planning	12
2.3.2 The evolution of Business Continuity Planning	13
2.3.3 Business Continuity Planning today	14
2.3.4 An explanation of various continuity planning concepts	15
2.4 The need for BCP within organisations	17
2.4.1 Business Continuity Planning benefits.....	18
2.4.2 Legal responsibilities.....	19
2.5 Conclusion	21
Chapter 3 Business Continuity Planning Today.....	22
3.1 Introduction.....	22
3.2 Methodologies: A general perspective	22
3.3 Characteristics of methodologies	23
3.4 A general overview of Business Continuity Planning methodologies.....	25
3.5 A discussion of current methodologies	26
3.5.1 Methodology 1	26
3.5.2 Methodology 2.....	30
3.5.3 Methodology 3	34

3.5.4 Methodology 4.....	36
3.6 Conclusion.....	42
Chapter 4 Business Continuity Planning in Small to Medium Sized Organisations.....	43
4.1 Introduction.....	43
4.2 Classification of small and medium sized organisations.....	43
4.2.1 Classification according to workforce size.....	44
4.2.2 Classification according to annual revenue and capital assets	45
4.3 Characteristics of smaller organisations that affect BCP	46
4.4 Business Continuity Planning: A small business perspective	50
4.4.1 Financial and budgetary BCP repercussions	50
4.4.2 Staff size and innovative effects	51
4.4.3 Job creation and SME environments.....	53
4.4.4 The effects of SME conduct and management structure.....	53
4.4.5 The effects of dealing with larger organisations.....	55
4.4.6 The effects of organisational infrastructure.....	56
4.5 Conclusion	57
Chapter 5 A Detailed Business Continuity Planning Methodology.....	59
5.1 Introduction.....	59
5.2 The Project Planning Phase	60
5.2.1 Ensure top management commitment	60
5.2.2 Conducting a high level awareness exercise	62
5.2.3 Establish a business continuity planning committee.....	63
5.2.4 Determine project prospects	64
5.3 The Business Impact Analysis Phase.....	65
5.3.1 Identifying critical business processes	65
5.3.2 Identifying failure scenarios	66
5.3.3 Calculate criticality factors.....	68
5.3.3.1 Determining the Recovery Time and Point Objectives.....	68
5.3.3.2 Determining the costs of impact.....	69
5.3.4 Prioritising business processes.....	70

5.3.5	Identifying supporting resources.....	72
5.4	The Business Continuity Strategies Phase	73
5.4.1	Identifying backup strategies	74
5.4.1.1	Backing up data.....	74
5.4.1.2	Transporting data offsite.....	75
5.4.2	Identifying processing alternatives	76
5.4.3	Identifying user holding strategies	79
5.4.4	Insurance coverage review	79
5.4.5	Public relations.....	80
5.5	Continuity Strategy Implementation	83
5.5.1	Identifying emergency response procedures	84
5.5.1.1	Emergency notification procedures.....	84
5.5.1.2	Plan invocation procedures.....	84
5.5.2	Writing process continuity an recovery procedures.....	85
5.5.2.1	Process continuity procedures.....	85
5.5.2.2	IT recovery procedures	85
5.5.3	Establish continuity planning team structure.....	86
5.5.3.1	The management recovery team	86
5.5.3.2	The administrative recovery team	87
5.5.3.3	The user recovery team.....	87
5.5.3.4	The technical recovery team	88
5.6	The Continuity Training Phase	89
5.6.1	Introductory awareness training.....	89
5.6.2	Detailed awareness training.....	89
5.7	The Continuity Testing Phase.....	90
5.7.1	Developing test plans	90
5.7.2	Conducting the tests	91
5.7.2.1	Hypothetical tests	91
5.7.2.2	Component tests	92
5.7.2.3	Module tests	92
5.7.2.4	Full tests.....	93
5.7.3	Analysing the test results.....	93
5.7.3.1	Conducting a debriefing session	94
5.7.3.2	Writing a test report.....	94

5.8	The Continuity Plan Maintenance Phase.....	95
5.9	Conclusion.....	96
Chapter 6	A Cyclic Approach to Business Continuity Planning.....	99
6.1	Introduction.....	99
6.2	A cyclic implementation.....	100
6.3	A discussion of the four BCP cycles.....	101
6.3.1	The backup cycle	103
6.3.1.1	The Project Planning phase.....	103
6.3.1.2	The Business Impact Analysis (BIA) phase	104
6.3.1.3	The Business Continuity Strategies phase	104
6.3.1.4	The Continuity Strategies Implementation phase	105
6.3.1.5	The Continuity Training phase.....	105
6.3.1.6	The Continuity Testing phase	105
6.3.1.7	The Continuity Plan Maintenance phase	106
6.3.2	The disaster recovery cycle	106
6.3.2.1	The Project Planning phase.....	107
6.3.2.2	The Business Impact Analysis (BIA) phase	107
6.3.2.3	The Business Continuity Strategies phase	108
6.3.2.4	The Continuity Strategies Implementation phase	108
6.3.2.5	The Continuity Training phase.....	108
6.3.2.6	The Continuity Testing phase	109
6.3.3	The contingency planning cycle	109
6.3.3.1	The Project Planning phase.....	110
6.3.3.2	The Business Impact Analysis (BIA) phase	110
6.3.3.3	The Business Continuity Strategies phase	110
6.3.3.4	The Continuity Strategies Implementation phase	110
6.3.3.5	The Continuity Training phase.....	111
6.3.3.6	The Continuity Testing phase	111
6.3.4	The continuity planning cycle.....	112
6.3.4.1	The Project Planning phase.....	112
6.3.4.2	The Business Impact Analysis (BIA) phase	112
6.3.4.3	The Business Continuity Strategies phase	112

6.3.4.4	The Continuity Strategies Implementation phase	113
6.3.4.5	The Continuity Training phase.....	113
6.3.4.6	The Continuity Testing phase	113
6.4	Conclusion.....	114
Chapter 7	Maintaining a Living and Dynamic Business Continuity Plan....	115
7.1	Introduction.....	115
7.2	Organisational changes affecting BCP.....	115
7.2.1	Changes in personnel	116
7.2.2	Changes in hardware and software	118
7.2.3	Changes in business processes.....	120
7.2.4	Changes in vendors and suppliers.....	121
7.2.5	Changes in corporate policies and legislation	122
7.2.6	Changes in the location of organisational facilities	123
7.3	Conclusion.....	124
Chapter 8	Motivation and Continuous BCP Readiness of Employees.....	126
8.1	Introduction.....	126
8.2	Business Continuity Planning and employee readiness	126
8.2.1	Involve employees in plan maintenance	127
8.2.2	Electronic Communication Systems and awareness	128
8.2.3	Using incentives to motivate employees	129
8.2.4	Ensuring readiness through regular scenario training.....	130
8.2.5	Utilising job enrichment as motivational mechanism.....	130
8.2.6	Utilising job redesign as motivational mechanism	131
8.2.7	Eliminate demotivator factors within the organisation	133
8.3	Conclusion.....	134
Chapter 9	BCP Cyclic: A Prototype Implementation of the	
Cyclic Approach.....		135
9.1	Introduction.....	135
9.2	Adhering to the specifications of the cyclic approach	136
9.3	Technical decisions concerning the BCP Cyclic application	136

9.3.1	Programming language motivation.....	137
9.3.2	Information storage and the choice of a database.....	137
9.4	Design decisions for the BCP Cyclic application.....	138
9.4.1	User interface design.....	138
9.4.2	Keeping track of the information gathering progress.....	140
9.4.3	Assisting the user in information gathering activities.....	142
9.4.4	Guiding the user towards the right choices.....	143
9.5	Possible improvements for the BCP Cyclic prototype.....	144
9.5.1	Lack of printing capability.....	144
9.5.2	Representation and gathering of non-standard information.....	145
9.6	Conclusion.....	146
 Chapter 10 Case Study		147
10.1	Introduction.....	147
10.2	Case study objectives.....	147
10.3	The nature of the case study.....	148
10.4	The case study process.....	148
10.5	Findings and suggestions.....	149
10.6	Conclusion.....	151
 Chapter 11 Conclusion		152
11.1	Introduction.....	152
11.2	Summary.....	153
11.3	Limitations of dissertation.....	156
11.4	Future research directions.....	157
11.5	Conclusion.....	157
 List of References.....		159
 Annexure A.....		170
BCP Cyclic System Documentation		

Annexure B	199
BCP Cyclic User Manual	
Annexure C	238
BCP Cyclic Prototype Output	
Annexure D	255
Paper submitted to Information Management & Computer Security – ‘A <i>Cyclic Approach to Business Continuity Planning</i> ’	

List of Figures

Chapter 2

2.6 Business Continuity Planning, Contingency Planning and Disaster Recovery Planning relationship.....	16
--	----

Chapter 5

5.10 Time Tolerance and Cost of Impact graph.....	72
---	----

Chapter 6

6.5 A cyclic approach to Business Continuity Planning.....	101
--	-----

Chapter 9

9.7 An example of the BCP Cyclic MDI.....	139
9.8 A cycle progress window.....	140
9.9 An information gathering wizard progress indicator.....	141
9.10 An example of on-screen text guidance.....	143
9.11 A warning message.....	144

List of Tables

Chapter 5

5.11 Tangible and Operational Cost Values.....	70
5.12 Intangible Cost Values	70
5.13 RTO Values	71
5.14 A summary of SME characteristic effects.....	97

Chapter 11

11.1 Methodology subdivision by means of the Cyclic Approach.....	154-156
---	---------

Introduction

1.1 Background

The Information Technology (IT) industry has grown and has become an integral part in the world of business today. The importance of information, and IT in particular, will in fact only increase with time (von Solms, 1999). For a large group of organizations computer systems form the basis of their day-to-day functioning (Halliday, Badendorst & von Solms, 1996).

These systems evolve at an incredible pace and this brings about a greater need for securing them, as well as the organizational information processed, transmitted and stored. This technological evolution brings about new risks for an organization's systems and information (Halliday et. al., 1996). If IT fails, it means that the business could fail as well, creating a need for more rigorous IT management (International Business Machines Corporation, 2000). For this reason, executive management must be made aware of the potential consequences that a disaster could have on the organisation (Hawkins, Yen & Chou, 2000).

A disaster could be any event that would cause a disruption in the normal day-to-day functioning of an organization. Such an event could range from a natural disaster, like a fire, an earthquake or a flood, to something more trivial, like a virus or system malfunction (Hawkins et. al., 2000). During the 1980's a discipline known as Disaster Recovery Planning (DRP) emerged to protect an organization's data centre, which was central to the organisation's IT based structure, from the effects of disasters. This solution, however, focussed only on the protection of the data centre. During the early 1990's the focus shifted towards distributed computing and client/server technology. Data centre protection and recovery were no longer enough to ensure survival. Organizations needed to ensure the continuation of their mission critical processes to support their continued goal of operations (IBM Global Services, 1999)

Organizations now had to ensure that their mission critical functions could continue while the data centre was recovering from a disaster. A different approach was required. It is for this reason that Business Continuity Planning (BCP) was accepted as a formal discipline (IBM Global Services, 1999). To ensure that business continues as usual, an organization must have a plan in place that will help them ensure both the continuation and recovery of critical business processes and the recovery of the data centre, should a disaster strike (Moore, 1995).

Wilson (2000) defines a business continuity plan as “a set of procedures developed for the entire enterprise, outlining the actions to be taken by the IT organization, executive staff, and the various business units in order to quickly resume operations in the event of a service interruption or an outage”. With markets being highly competitive as they are, an organization needs a detailed listing of steps to follow to ensure minimal loss due to downtime. This is very important for maintaining its competitive advantage and public stature (Wilson, 2000). The fact that the company’s reputation is at stake requires executive management to take continuity planning very serious (IBM Global Services, 1999). Ensuring continuity of business processes and recovering the IT services of an organization is not the sole responsibility of the IT department. Therefore management should be aware that they could be held liable for any consequences resulting from a disaster (Kearvell-White, 1996).

Having a business continuity plan in place is important to the entire organization, as everyone, from executive management to the employees, stands to benefit from it (IBM Global Services, 1999). Despite this, numerous organizations do not have a business continuity plan in place. Organizations neglecting to develop a plan put themselves at tremendous risk and stand to lose everything (Kearvell-White, 1996).

1.2 Problem Statement

A large percentage of organizations today fail to recognise the importance of BCP and the impact a disaster could have on their day-to-day functioning. For organizations that fall into the category of small or medium, the development of a business continuity plan could prove even more difficult, even if it does realise the importance of such a plan.

Literature concentrating on the development of a business continuity plan seldom concentrates on the development of continuity plans for smaller organisations. These smaller organisations usually do not have the same resources available as large organisations and as a result the development of a continuity plan becomes increasingly difficult (Weems, 1999).

BCP methodologies are normally very comprehensive and detailed, requiring specialised resources to implement and maintain. The organisational structure and IT infrastructure of small to medium sized organisations usually differ a lot from those of large organisations. For this reason one can argue that the BCP methodologies utilised in large organisations might not be ideal for implementation in smaller organisations. One could further argue that the difference in BCP methodologies, addressing smaller companies, would be mostly implementation based. For that reason an implementation method for BCP methodologies that will ensure simple implementation would prove useful.

Furthermore, once a BCP methodology has been implemented and a business continuity plan created, it must be continually maintained. This is to ensure that the plan reflects the organisation and all organisational changes. Organisations therefore need a way to keep plans dynamic. Continuous employee readiness is another important factor for organisations. They need to keep employees continually ready to perform their BCP duties to ensure an effective and efficient recovery process.

1.3 Objectives

The primary objective of this study is to develop an implementation approach for BCP methodologies that will be aimed specifically at the implementation of methodologies suited to small to medium sized organisations.

Secondary objectives will be:

- Developing a well-structured and complete BCP methodology based on a study on various existing BCP methodologies along with their strong and weak points. This methodology will be scalable so that it can be implemented in both large and small organisations.

- Developing a prototype implementation that utilises the proposed implementation approach along with the developed BCP methodology to create a complete business continuity plan based on the specific organisational requirements.
- Developing a set of suggestions that will ensure a dynamic business continuity plan as well as continued employee BCP readiness.

1.4 Research Methodology

In order to complete this study and develop a BCP implementation approach and detailed methodology, various options will be used to gather the required information. Firstly, a thorough literature study will be conducted covering all aspects of BCP that are relevant to this study. An investigation will be done into the criteria used to distinguish large organisations from small and medium sized organisations as well as the characteristics of smaller enterprises that could have an effect on the continuity planning process.

Once information has been gathered, existing continuity planning methodologies will be studied and evaluated in order to determine their various strengths and weaknesses. This will allow for the development of an improved methodology. These existing methodologies will then be investigated thoroughly and argumentative techniques will be used to select and identify those steps necessary to ensure that the new methodology will be complete and effective in producing a virtually flawless business continuity plan.

Once the implementation approach and BCP methodology have been completed, a model, depicting the approach graphically, will be produced. This is to describe the entire continuity planning process and methodology implementation in detail.

In turn, the resultant model will help in the development of a working prototype that will demonstrate how the methodology can efficiently be used to develop a business continuity plan for small to medium sized organisations.

After the prototype development is complete, it will be tested through making use of a case study involving a small or medium sized organisation with the sole purpose of establishing whether it can effectively be used to produce a business continuity plan. The effects and

results from this case study will be interpreted and discussed in detail. Recommendations regarding the proposed methodology and implementation plan will be made based on the results of the case study.

1.5 Structure of Dissertation

In section 1.1, a brief introduction was given to the importance of information security and the need for BCP within organisations. Both these topics will be discussed further in chapter 2 which is entitled “Information Security: An Introduction”. It will attempt to discuss the role of BCP in organisations today. The terms Business Continuity Planning, Contingency Planning and Disaster Recovery Planning will be clearly defined and distinguished between, with the emphasis on availability and continuity of business processes.

The next chapter will be entitled “Business Continuity Planning Today” and will discuss four current BCP methodologies. It will also critically evaluate them in an effort to determine the criteria required for producing a reasonably effective methodology for small to medium sized organisations. Once the existing methodologies have been studied, chapter 4 will examine small, medium and large organisations. It will attempt to distinguish between these three types of organisations and identify characteristics that will have an effect on BCP within the organisation. It will also attempt to identify how these characteristics affect the business and what needs to be done differently than in large organisations with respect to continuity planning. The chapter will be entitled “Business Continuity Planning in Small to Medium Sized Organisations”.

The fifth chapter will be entitled “A Detailed Business Continuity Planning Methodology” and will discuss the development of a BCP methodology for small to medium sized organisations. It will be based on previously reviewed methodologies as well as the criteria that distinguish small to medium sized organisations from large organisations. Chapter 6 will complement chapter five by discussing an implementation approach for BCP methodologies. It will be entitled “A Cyclic Approach to Business Continuity Planning” and will discuss the partitioning of methodology phases into four progressive development cycles. This will be based on organisational requirements with respect to continuity planning.

The seventh chapter is entitled “Maintaining a Living and Dynamic Business Continuity Plan” and will discuss how an organisation can ensure that all organisational changes will be reflected in the business continuity plan, thus ensuring that the plan is maintained. Chapter eight will be entitled “Motivation and Continuous BCP Readiness of Employees”. It will propose techniques to ensure that those employees involved in the continuity planning process stay continually ready despite a changing and dynamic organisational environment.

The ninth chapter will be entitled “BCP Cyclic: A Prototype Implementation of the Cyclic Approach”. It will discuss the development of a prototype implementing the previously developed methodology allowing for the creation of a complete business continuity plan. Chapter ten will discuss a case study performed using the prototype discussed in the previous chapter.

The eleventh and final chapter is a conclusion chapter that will contain a summary of the aspects as discussed in the previous chapters. It will also provide an overview of the entire study, contain some conclusive remarks and discuss the possibility for further research.

Annexure A will provide the system documentation for the BCP Cyclic prototype. This documentation will include several technical aspects related to the prototype.

In Annexure B, the user documentation for the prototype will be discussed. This will serve to guide users through the use of the aforementioned software package.

Annexure C will comprise of output generated by the BCP Cyclic prototype, based on input from the case study.

Annexure D will include a research paper entitled “A Cyclic Approach to Business Continuity Planning” that resulted from this research project.

Information Security: An Introduction

2.1 Introduction

Computer and network environments are developing at an incredible pace. Along with this, information security is growing as well and becoming more complex as technology advances. To ensure the continuation of mission critical business processes, information security has to support these processes and employees concerned with information security need to understand how these business processes operate (Yngström & Carlsen, 1997, p. 3-4). It has been indicated by surveys and statistical evidence that senior management has, until recently, not paid much attention to information management and security. Advances in distributed systems, especially the Internet, have caused management to focus their attention predominantly on organisational threats and the possible effects they might have (Yngström & Carlsen, 1997, p. 7-8).

Management is becoming increasingly aware that business functions should be available at all times. Organisations nowadays operate in environments where operations have to be available twenty-four hours a day for seven days a week. They should, therefore, try to establish how a disaster could affect their operations. Further, they also need to determine what needs to be done to ensure continuous operations (Douglas, 1998). With natural and other disasters constantly looming, organisational information is constantly at risk. A proactive approach is needed to ensure continuous availability of computer systems (Underwood, 1998).

Both disaster recovery experts and business recovery practitioners agree that simply planning for recovery of the IT department and its systems is not adequate to ensure the survival of an organisation (Karakasidis, 1997). Organisations should also keep in mind that one of the main objectives of BS7799 is to ensure business continuity (BS7799-1, 1999, p. 75).

This chapter will, therefore, discuss the importance of information security to an organisation and also show how it relates to Business Continuity Planning (BCP). It will specifically show how important the continuation of business functions is to ensure survival after a disaster.

2.2 Information Security

Information plays a crucial role in the day-to-day functioning of practically any organisation. It is a vital asset that adds value to an organisation and its business processes (BS7799-1, 1999, p.1). In fact, it has been at the centre of business for decades. Companies are under an incredible amount of pressure from their competitors to perform in a global market. The information they possess is no longer only used by employees, but by customers and partners as well. These users expect continuous availability of, and instantaneous access to, organisational information (McAnally, P., DiMartini, B., Hakun, J., Lindman, G. & Parker, R., 2000).

This section will firstly concentrate on the role of information and information security in an organisation, stipulating why it is required along with other relevant aspects. Secondly, it will discuss three pillars on which information security rests. It will be shown how these pillars, namely confidentiality, integrity and availability, support the protection of organisational information. Specific reference will be made to the continuous availability of information.

2.2.1 The importance of information security

The objective of this sub-section is to emphasise the role that information security plays in the day-to-day functioning of an organisation. Focus will be placed on the evolution of information security and computers in general, as well as the effect that security breaches could have on the organisation. Management roles and their attitude towards information and its protection will be discussed as well.

Information security requirements have gone through significant changes in the last few years. Before data processing equipment started to play such a crucial role, information was primarily protected through physical and administrative

techniques. With the introduction of the computer, it became clear that automated tools were now needed to protect files and other important information. A second important change was the introduction of the distributed computing environment and the use of networks for information transmission (Stallings, 1995).

Information and the business processes, systems and networks that use this information are extremely important to an organisation. Protection of the information is essential to ensure that the business has a competitive edge and maintain cash flow and commercial image, while complying with legal requirements. Unfortunately, organisations are constantly faced with threats to their information (BS7799-1, 1999, p.1). This information and Information Technology (IT) is playing a vital role in the world of business today and this importance of IT is rapidly growing (von Solms, 1999, p50).

IT and business are almost impossible to separate in today's technologically advanced world. This unique combination not only has the role of enhancing an organisation's efficiency and effectiveness, but IT departments also take initiative in leading the organisation into innovative industry structures and markets. (IBM Global Services, 2000). While technology is developing at an incredible pace, the need to secure systems is increasing just as rapidly. The increased use of computer systems and networks, especially the Internet, provides numerous opportunities for computer crime. (Halliday, Badenhorst & von Solms, 1996, p. 19)

Securing information and information systems is no longer only the responsibility of the IT department. The organisation's senior management also has to take part in ensuring that effective security measures are in place to protect information. Management has to have a good understanding of the organisation's situation concerning information security as well as the quality of the information security processes.

They should preferably understand how these processes relate to business management and the continuity of the organisation (Eloff, Labuschagne, von Solms & Verschuren, 1999). The need for proper information security measures in all

organisations cannot be questioned in today's day and age. Precisely what is meant by information security will be discussed next.

2.2.2 The three pillars of information security

This sub-section is primarily aimed at discussing the importance of ensuring confidentiality, integrity and especially availability of information. These three factors will be discussed along with their relevance to information security and the organisation.

Information, as mentioned previously, is an important corporate asset, along with the systems and networks processing it. To ensure that an organisation maintains its competitive edge, the information must be kept confidential, accurate and continuously available. Keeping this in mind, information security can therefore be classified as a combination of the following three factors (BS7799-1, 1999):

- Confidentiality : Ensuring that those who are unauthorised to access information are prevented from doing so
- Integrity : Ensuring that both the information and the methods by which it is processed, are accurate and complete
- Availability : Ensuring that those users who have authorization to access information, are able to do so when required

To ensure confidentiality, integrity and availability, information security comprises mechanisms and procedures for exactly this purpose. (Leiwo, Kajava, & Nesland, 1994). To identify the appropriate technical mechanisms, three factors need to be considered. These are the functionality, assurance of correctness as well as effectiveness of these mechanisms. This means that such mechanisms should sufficiently protect an organisation's information, be properly implemented and be effective in accomplishing what they are intended for (von Solms, 1999, p52).

Besides identifying and implementing these mechanisms, organisations must furthermore educate users and other employees on issues, such as the importance of information security, the usage of information protection mechanisms, information classification and possible information risks. (Leiwo, Kajava, & Nesland, 1994). This will ensure sufficient protection of organisational information should any risks materialise.

Any information security risks could cause possible alteration, destruction, or disclosure of information, as well as a disruption in information processing. Information security provides protection to prevent these risks from affecting the information and therefore the organisation (Leiwo, Kajava, & Nesland, 1994). Should any such risks materialise, the confidentiality, integrity and availability of information could easily be compromised. Although ensuring confidentiality and integrity is important, the availability component of information security is of greater importance with respect to this study.

Organisations nowadays are competing on a global scale and require high availability levels of information technology resources and services (Glorioso & Desautels, 1999). The following section will therefore address the process of information availability and its importance to an organisation's survival.

2.3 Business Continuity Planning (BCP)

The majority of organisations today realise that they cannot function without the continued availability of their information technology resources (McKinney, 2000). Therefore, they are constantly at risk due to the threat posed to their information by natural disasters and other unforeseen events. As they become more dependent on continuous availability of their information, organisations have to take measures to ensure that business continues as usual following some disaster or event (Underwood, 1998).

No organisation is immune to the effect of disasters and these disasters might prove fatal to its survival. Fires, floods and explosions usually come to mind when the word disaster is mentioned, but virus infections, unreliable data, and hardware and software failures are, however, a more common occurrence. A large number of organisations affected by a

disaster do not have procedures in place in order to effectively deal with it (Boddington, 1998). Therefore, companies may experience major survival threats if they do not have some form of continuity procedures in place to help them through the normalization period. In the past such procedures served primarily to ensure that the data centre of an organisation kept downtime to a minimum. These procedures to recover the data centre were generally known as disaster recovery procedures (IBM Global Services, 1999).

As technology evolved and became more sophisticated, organisations started to rely a great deal on the availability of their systems and technology. As continuous availability was now important, Disaster Recovery Planning (DRP) evolved into BCP. The aim of BCP is to make data centre downtime transparent to those outside the organisation (King, 2000). Many companies, especially those that are Web based, must operate twenty-four hours a days, seven days a week and BCP helps these companies to achieve a state of complete business continuity (IBM Global Services, 1999).

For many organisations the World Wide Web is increasing in popularity as a tool to conduct business. This unfortunately means that disaster tolerance and recovery is also growing in importance for these organisations. A disaster could mean that an organisation would no longer be accessible to their customers, employees and suppliers. This could in turn mean major losses in income and valued customer support (Florendo, Martens, Middlebrooks, Romanyschyn & Solter, 1998).

The rest of this section will discuss disasters and the effect that they might have on an organisation and its business functions. Secondly, the evolution of BCP will be discussed along with BCP as it is practiced today. The final sub-section will elaborate on various concepts as used in BCP and clearly define the difference between the various concepts.

2.3.1 Disasters and Business Continuity Planning

“A disaster may be any accidental, natural or malicious event which threatens or disrupts normal operations, or services, for sufficient time to affect significantly, or to cause failure of, the enterprise” (Hassim, 2000, p. 2). Business disasters need not be to the extent of a hurricane to pose a serious threat to an organisation.

Disasters are not bound to time or location either. The majority of disasters are as a result of unplanned events in and around the working environment. Such disasters could be as trivial as neglecting to save an important file, a complete network failure, losing installation backup disks or the loss of the original copy of an important document. They could furthermore include the compromising of an online transaction processing web site or the deletion of critical files by a new employee (Wilson, 2000).

Such unfortunate mishaps, as described in the previous paragraph, are much more likely to occur than those of greater magnitude such as fires, storms or social unrest. Computer virus infections and equipment failure are after all more common occurrences (Wilson, 2000). Such business disruptions, whether they are isolated or community wide, have shown that a need exists for well designed and tested service disruption plans to be in place. Such a plan is to ensure that an organisation's assets, operations, commitments and relationships throughout the organisation are kept in tact. This is important for ensuring business continuity (Moore, 1997). These disasters usually occur at the most inappropriate times. They are unpredictable and therefore should be accepted as a reality in any organisation and consequently require an adequate level of preparedness (Campbell, Danton, Hodgetts, Melamed & Spagnolo, n.d.).

Nowadays the outages caused by these risks are measured in hours and no longer in days. For e-business, it is more important to be able to handle sudden peaks in web traffic than worrying about natural disasters. Electronic transactions take place at an incredible rate. The work and business that could be done in an hour by far exceeds that of previous decades. What was previously seen as a trivial event, for example a defective hard disk or a software malfunction, could today be seen as being of the same magnitude as effects caused by a natural disaster some decades ago (IBM Global Services, 1999).

2.3.2 The evolution of Business Continuity Planning

During the 1980's a discipline known as Disaster Recovery Planning (DRP) was formally accepted and was aimed at protecting an organisation's data centre from

the effects of disasters. The data centre was central to the organisation's IT based structure at the time (IBM Global Services, 1999). However, the IT environments at present differ from the host-centric systems of two decades ago. Networks are more complex and consist of several servers and a large number of personal computers and peripheral devices. Already in the early 1990's organisations started abandoning the centralised approach with the advent of distributed computing and client/server technology (IBM Global Services, 2000).

This shift in technology also brought about a change in organisational functioning. Information technology became intertwined with the majority of business functions. Information essential to business survival was spread across the organisation and not found only in the data centre anymore. Critical business functions continuously access this critical information on a regular basis. Information technology has, therefore, become a critical component of business. It is no longer enough to safeguard information only, but the critical business processes as well (IBM Global Services, 1999).

Simply having a backup and recovery plan in place is not sufficient anymore. An effort should be made to ensure business continuity along with disaster recovery (IBM Global Services, 2000). Business continuity, therefore, involves not only the recovery of the IT infrastructure, but ensuring that information is continually available throughout the organisation. It also ensures that natural and other disasters do not disrupt the day-to day functioning of the organisation, allowing revenue-generating functions to continue (Ogorchock, 1998).

2.3.3 Business Continuity Planning today

The challenges that face continuity planners are escalating each day. Backup windows are becoming smaller and those operations that require continuous availability for twenty-four hours a day and seven days a week, are growing in size. The amounts of data to be recovered are ever increasing and applications used are changed regularly. Business continuity planners have to keep up with these dynamic changes (Gonzalez & Solter, 1999).

The objectives of BCP, namely data recovery and business continuity, remain unchanged. The obstacles, however, are becoming more difficult to overcome because of changes in technology (Eckert, 1999). The Internet is one such technology and it is starting to play an important role in both business and planning for continuity (Gonzalez & Solter, 1999).

The Internet has become a very important communications medium for ideas, information and business transactions. It is an essential tool for circulating information between organisations and to assist with critical business functions. As the Internet becomes more important, the loss of access to it also becomes more devastating (Gonzalez & Solter, 1999).

Organisations now realize that business functions on the Internet are to be continually available to ensure revenue flow, customer service and employee productivity. The sheer amount of people accessing organisational information through the Internet today has increased considerably. This information is available to partners, employees, customers and suppliers but unfortunately to hackers as well. Organisations nowadays have to plan for and counter the interruptions caused by either malevolent or inadvertent acts orchestrated over the Internet (Gonzalez & Solter, 1999).

2.3.4 An explanation of various continuity planning concepts

Various definitions of BCP are available. Glenn (2002) feels that this BCP process has two parts to it. Firstly it ensures that an organisation can continue business as usual when disaster strikes. Secondly, it caters for business recovery to a state similar to that preceding the disaster. To better understand these two components of BCP, the concepts Contingency Planning and DRP will be discussed in this section.

The definition of DRP was originally intended for operations established to minimise data centre downtime. To accomplish this, agreements with other companies and vendors were set up to protect against the effects of disasters (King, 2000). Today DRP is seen as the active component of continuity planning and is

only one of the deliverables of the planning process. As the name states, the focus of DRP is the recovery of the IT facilities and all related and required functions. The recovery timeframe differs from one organisation to the other and should be determined by the organisation itself. The disaster recovery component of BCP is therefore aimed at producing detailed recovery plans to ensure that the organisation can react appropriately in disaster situations (Hassim, 2000).

The aim of Contingency Planning is to make provision for continuing business processes in a disaster situation while recovery is taking place (Glenn, 2002). It can be defined as the process of examining an organisation’s critical functions, identifying the possible disaster scenarios and developing procedures to address these concerns (Rubin, 1999, p. 73). Contingency plans should therefore be developed and put into practice to give an organisation the assurance that business processes can continue and be restored within the given timeframes (BS7799-1, 1999).

Keeping the previously discussed definitions in mind, BCP can be defined as a complete process of developing measures and procedures to ensure an organisation’s disaster preparedness. This includes ensuring that the organisation would be able to respond effectively to a disaster and that their critical business processes can continue as usual (Business Continuity Preparedness, 2002). According to Glenn (2002) BCP includes, amongst other things, procedures to continue business processes and procedures to quickly restore operations in the event of a disaster. Although many authors differ on the precise and clear distinction between the above-mentioned concepts, their inter-relationship, with respect to this study, can be depicted as follows:

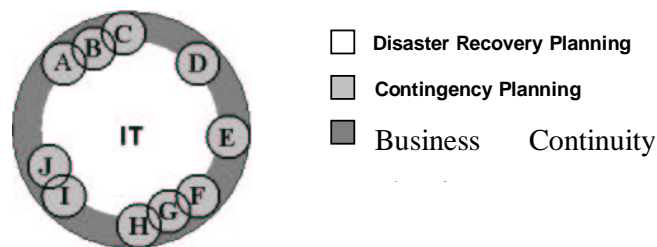


Figure 2.1: Business Continuity Planning, Contingency Planning and Disaster Recovery Planning relationship

In figure 2.1, the innermost circle, labelled IT, represents an organisation's IT infrastructure and the services it provides. The DRP component focuses mainly on the recovery of this infrastructure and services. The small light grey circles labelled A to J represent the business processes an organisation might have. These are dependent on the services provided by the IT infrastructure and, in some cases, on one another, as depicted in the figure. For each of these processes a plan must exist to ensure their continuation following a disaster. This is what Contingency Planning aims to accomplish.

Finally, the outermost dark grey circle represents BCP, i.e. it combines the disaster recovery plans for the IT infrastructure with the contingency plans for the individual business processes and adds some organisational activities that need to be completed, like a formal public relations exercise and insurance requirements identification.

As shown in the above section, BCP has evolved considerably over the last few years. This is mostly due to the effects of disaster and other unplanned events that threaten business continuity. Disasters are constantly looming and, therefore, organisations must preferably implement a business continuity plan. As indicated above, this process of continuity planning includes both disaster recovery and process continuity procedures. These two aspects are essential to ensure an overall state of business continuity. The next section will further elaborate why BCP is so important for organisations.

2.4 The need for BCP within organisations

Without a tested and continually updated business continuity plan an organisation leaves itself open to a variety of threats. Simply ignoring the possibility of disasters striking is not an option. Organisations are competing globally and are extremely dependent on their information systems. Taking the time to implement a continuity plan prior to a disaster could mean the difference between business continuity and recovery, or failure. Organisations should know that every minute of downtime increases losses and associated expenses (Wilson, 2000).

According to the Vistastor Corporation (2002), 43 percent of organisations that are affected by disasters close almost immediately and of those that manage to survive, 29 percent close within a matter of two years. Further statistics indicate that a company that experiences IT infrastructure downtime of more than ten days will never recover completely. Of these organisations 50 percent will cease to operate within five years of the occurrence of the disaster. Lastly, estimates show that one in every five hundred organisations will experience a severe disaster at least once a year (Vistastor Corporation, 2002)

Except for the costs and other business drawbacks that are associated with disasters, there are also other reasons for initiating a BCP project. This section will firstly concentrate on the benefits of continuity planning. It will explain what the presence of a continuity plan could mean for an organisation. Secondly, the legal consequences of not having a plan in place will be discussed.

2.4.1 Business Continuity Planning benefits

For a large number of organisations their main goal is survival and guaranteeing a profit at the end of the day. Keeping this in mind, defining the business benefits of continuity planning is relatively simple. BCP could be seen as being equivalent to liability insurance, allowing an organisation to function, realising that a major disaster will not result in its demise. Insurance alone can unfortunately not ensure business continuity and does not cover intangible costs resulting from disruptions to business (Devargas, 1999).

In a disaster situation a continuity plan focuses attention on important business issues. If the plan is properly constructed, it will help even those who are inexperienced to carry out the required recovery and continuity procedures. The fact that an organisation has a continuity plan in place already gives management the assurance that they are equipped to handle a disaster and will not be held liable for negligence (Devargas, 1999). Some of the more common and important benefits are assurance that business will continue as usual after a disaster has struck and the prevention of a loss in market position (Hassim, 2000). The protection of

organisational assets also plays a role in the justification of a continuity plan (Devargas, 1999).

Further benefits include the reduction of decisions that need to be made in crises situations as well as the elimination of confusion and mistakes during the crisis period. Reliance on key individuals in the continuity planning process is also minimised (Devargas, 1999). Even if the plan is never used, its existence will ensure that management's and organisation employees' knowledge about the functioning of the organisation and its processes increase. This is due to the ongoing training and maintenance process. Potential weaknesses are furthermore pointed out and the appropriate actions are taken to minimise the risk. Even if the plan is never activated, potential loss situations are ultimately avoided (Hassim, 2000).

Therefore, it is essential that an organisation has a well-tested and consistently maintained business continuity plan in place. Those who lack such a plan are taking an immeasurable risk, which can be construed as extremely negligent. The next sub-section will focus on the legal implications attached to the lack of implementation of such a business continuity plan.

2.4.2 *Legal responsibilities*

Problems that are of a legal nature, along with disasters, pose a serious threat to organisations if they do not realise that these problems could be avoided. Simply ignoring legal issues could prove to be an expensive and time-consuming mistake. Legal problems could include a variety of possibilities such as workplace safety, contract disputes, copyright disputes etc. Therefore, besides the benefits provided by BCP, an organisation also has these legal responsibilities to take into account. They must ensure that a continuity plan satisfies all legal requirements before it is accepted.

To accomplish the aforementioned a continuity plan must satisfy the following requirements:

- Statutory requirements : Organisations need to be aware of the various constitutional laws and regulations they have to adhere to. An example is the UK Fire Precautions Regulations which implements directives that deal with the minimum workplace safety requirements (Devargas, 1999).

- Contractual requirements : Most organisations have contracts to uphold and some of these contracts require continuous availability of services provided by the organisation. If their continuity plans are not up to standard they could be facing a lawsuit for not providing the agreed upon services or products within the specified timeframe (Devargas, 1999).

- Corporate governance requirements : The King report on Corporate Governance for South Africa stipulates that an organisation must ensure that it has recovery and continuity procedures in place. The report furthermore specifies that the board of directors could be held accountable if procedures are not correctly implemented (King Committee on Corporate Governance, 2001).

The above section discussed the reasons why a company should give serious thought to implementing a business continuity plan. Not only was it seen that BCP has a variety of obvious benefits but that organisations are often required by law to make sure that they will be able to continue business in the wake of disaster.

2.5 Conclusion

Information plays a vital role in the world of business today. It is not only important to employees, but to an organisation's customers and shareholders as well. Information is crucial in ensuring that an organisation keeps its competitive edge. In today's e-business world, information has to be available twenty-four hours a day and seven days a week to guarantee success. To accomplish this the information and the associate resources should be well protected.

Information used to be protected primarily through physical means, but due to technological advances the need arose for technological protection mechanisms. The introduction of distributed systems and networks also made the protection of information more challenging. It is imperative that an organisation ensures the confidentiality, integrity and availability of its information. Availability of information is of special importance to ensure the continued existence of an organisation. For this reason BCP was discussed as a tool to enhance availability to an acceptable level.

The aim of BCP is to help an organisation to continue functioning while the IT department is recovering after a disaster. In the past, organisations concentrated solely on disaster recovery, but these procedures did not ensure the continuation of business processes. For this reason DRP evolved into BCP, which includes procedures to ensure both business continuity and disaster recovery.

The next chapter will focus on the importance of methodologies, specifically for creating a sound business continuity plan. The chapter will also focus on four current BCP methodologies. These methodologies will be discussed and critically evaluated in order to identify the criteria that a good methodology comprises of.

Business Continuity Planning Today

3.1 Introduction

The previous chapter concluded by reiterating the importance of information security in the business world. Information has to be continuously available and protected to ensure that an organisation fully utilises this valuable asset. Methods for protecting information and the systems that use it have also changed considerably over the past few years due to advances in technology. Furthermore, the chapter also discussed Business Continuity Planning (BCP) as one of the tools to ensure continuous availability of information. The chapter then concentrated on the evolution of BCP from Disaster Recovery Planning (DRP). It also explained the different aspects associated with BCP, namely DRP and Contingency Planning.

This chapter will firstly focus on methodologies in general and their importance in research and especially BCP. Secondly, the chapter will contain a scrutiny and discussion of four well-known BCP methodologies. The aim is to identify those components essential to a successful BCP methodology as well as the advantages and disadvantages of each methodology. Once this chapter has been completed, a clear indication should be given of what an effective methodology must include.

3.2 Methodologies: A general perspective

A methodology can be defined as “a logical sequence of activities designed to efficiently guide us to the successful conclusion of a project” (Crannburn Innovative Software Solutions, 2002). A methodology could furthermore be seen as an outline on which to base a project. This is done in order to ensure that all the required steps are completed. One should, however, look at the objectives of a methodology to determine whether it is necessary to follow all methodology steps or only some. Based on the above, the success

of a methodology can be judged by the outcome of a project, i.e. whether the objectives, as mentioned above, were met (Veryard Projects Ltd., 2002).

Secondly, a methodology could be described as a collection of steps, tools and methods which one can use to complete a project. However, if a methodology is thought of in this way it could limit a project or its outcome. This is because any given project relies on the methodology to be complete and if the methodology is incomplete the resulting project could be left with flaws (Veryard Projects Ltd., 2002).

All projects are susceptible to a variety of risks that could negatively influence their outcome. A methodology, therefore, can be seen as a means to reduce the effect of these risks. Before producing a methodology it could be useful to assess the risks and determine how they might influence a project. Therefore, when designing a methodology it could be useful to keep these risks in mind, resulting in a more effective product. This would mean that the developed methodology would contain mostly strategies for solving the problems caused by these risks (Veryard Projects Ltd., 2002).

3.3 Characteristics of methodologies

The following section will discuss a selection of criteria that could be applied to methodologies, both in general and BCP methodologies, to determine how effective they are (Veryard Projects Ltd., 2002):

- **Effective** : The methodology should be evaluated to determine whether it accomplishes the task it is intended for, or produces the correct output for which it was intended. This is important to ensure that projects that follow the methodology turn out successful.

- **Efficient** : It should be ensured that all the steps contained in the methodology are absolutely necessary. All redundant steps and tasks should be omitted.

- Comprehensive : It should be made clear whether the methodology is restricted to specific situations or projects and if it is suited for any sized organisation. The size or complexity of projects it is suited for should also be clearly established.

- Accurate & reliable : It should be determined what risks are introduced if the methodology is implemented and what is done to ensure that these risks have minimum effect on the project.

- Flexible : The methodology should be easily updateable in case of any changes in technology or ideas concerning the project for which it is intended. It should also be easy to incorporate changes, learned through experience, into the methodology. Self-preservation mechanisms, to ensure that it stays relevant to the organisation, should also be present.

- Simple implementation : The target audience of the methodology should be well defined. It should be adaptable to the level of complexity of the project for which it is intended.

- Manageable : The methodology should preferably have guidelines that clearly define project management environments. This would include project management, coordination with other projects etc. It should also be defined when projects that make use of the methodology are considered successful and complete.

- Comprehensible : It should be simple to understand the methodology in order to easily determine whether each of the project phases is complete and relevant to the project.

- Well supported : Adequate support for that which is stated in the methodology should also exist in the form of appropriate tools, skills and services. If the necessary support does not exist, the prospects of development or acquisition of these tools, skills and services should be examined beforehand.

Now that the concept of a methodology has been defined and its characteristics identified, it is necessary to consider how methodologies relate to BCP. The following section will therefore concentrate on the use of and importance of methodologies in BCP.

3.4 A general overview of Business Continuity Planning methodologies

In the majority of organisations the adoption of some continuity planning standards or a methodology is essential to ensure that the developed continuity plans are consistent and comprehensive. Therefore, implementing such BCP methodology would guarantee that the creation of plans for the various business processes is coordinated effectively. In general, BCP methodologies have characteristics similar to conventional project management methodologies, as discussed in the previous two sections. As a result many organisations have developed BCP methodologies based on a combination of general methodology characteristics and specific organisational requirements (Heng, 1996).

A conventional business continuity plan usually includes various components that can be seen as crucial to the continuity planning process. The first is the conditions for plan activation. These refer to the procedures followed before a plan can be set in motion and include activities such as identifying parties involved and determining how to assess the situation. The second required component is the emergency procedures. These refer to the procedures to be performed immediately after disaster has struck. In general, they would include public relations and communicating with the relevant public authorities. The third component is the fallback procedures. These refer to the procedures for moving essential business processes to an alternate location as well as getting them up and running (BS7799-1, 1999).

Following the fallback procedures are the resumption procedures. These procedures describe what needs to be done in order to continue business functions as usual. A fifth required component is a maintenance schedule, which includes testing and maintenance procedures. Awareness and education activities follow. These are necessary to educate employees on the various business processes and how to ensure that these processes continue effectively during the recovery process. Finally, the methodology should include each individual's tasks as well as possible alternatives to replace employees if required (BS7799-1, 1999).

The above-mentioned discussion highlights typical components that should be present in any BCP methodology. The next section will discuss four BCP methodologies along with their benefits and shortcomings. The purpose of this is to identify the commonalities present in these methodologies along with other characteristics that could prove useful in designing a more complete methodology and should preferably be included in all BCP methodologies.

3.5 A discussion of current methodologies

As mentioned in section 3.4, following a BCP methodology is essential to ensure consistency and comprehensiveness of continuity plans. The problem is that a number of continuity planning methodologies are available today and differ quite extensively. The selection of a suitable methodology could therefore be a difficult process. This section will consequently examine four different methodologies currently in use and discuss the similarities and differences between them. By doing this it should become clear which phases and steps are common to all or most BCP methodologies.

3.5.1 Methodology 1

The first methodology is as presented by Devargas in a paper entitled "Survival is Not Compulsory". It comprises of six separate phases, namely the *project planning*, *vulnerability assessment*, *business impact analysis*, *strategy development*, *testing and exercising*, and *maintenance* phases. Along with the description of each phase, a listing of the deliverables for that specific phase is given in the discussion following (Devargas, 1999).

- Project Planning

The *project planning* phase attempts to verify the scope of the business continuity project. This includes setting up project schedules, determining what needs to be done and identifying factors that could delay the project or influence its success. The phase also involves appointing a decision board whose responsibility would be to guide all participants in the planning project and to give some direction to the project. Another task that needs to be completed during this phase is setting up schedules for conducting the Business Impact Analysis. According to Devargas, the deliverables of this specific phase are senior management commitment, the project infrastructure, project plans and awareness campaign plans (1999).

- Vulnerability assessment phase

During the *vulnerability assessment* phase all, or most of, the factors that could affect the completion of the business processes are identified. Business areas such as personnel, communications, operating procedures, backup and contingency planning, data, systems, access control and insurance should be reviewed for this purpose. Deliverables for this phase include assessment reports consisting of a worst-case scenario and recommended scenario, as well as a business health check report (Devargas, 1999). A business health check generally involves an operations audit to ascertain whether operations are performed as efficiently and effectively as possible (Scheur Management Group, 1999).

- Business Impact Analysis

The *business impact analysis* phase involves identifying those business processes most critical to the organisation, establishing the recovery time for each function and determining what the financial impact is that these functions may have on the organisation. The critical systems, processes and functions

must be identified along with the economic influence of disasters on each. The amount of time each business area is able to function effectively without access to critical systems and services should also be identified. Lastly, the recovery timeframes for critical systems must be determined as well. Devargas mentions that the deliverables are a business impact analysis report, a risk assessment review and business continuity plans (1999).

- Strategy Development

The *strategy development* phase aims to review the different options available for recovering those critical business processes as identified in the previous phase. An attempt is made to develop a collection of recovery alternatives as well as the operation plan that follows. Distinction is made between outages ranging from short to long term. The implementation of the recovery plan includes effecting changes to all procedures, negotiating contracts with recovery services vendors and defining recovery process teams. The tasks to be completed by these teams should also be defined. Deliverables include the disaster recovery procedures and training plans (Devargas, 1999).

- Testing/Exercising Program

During the *testing/exercising program* phase, the objectives and strategies for testing the developed continuity plans are identified. The organisational needs and culture play a big role in accomplishing this. These aforementioned objectives need to be agreed upon by all participants, but as soon as this has been done the tests can be developed and carried out. Once completed, the tests results can be evaluated. Deliverables include the results from the four types of tests (Checklist, Simulation, Parallel and Full interruption tests), business continuity tests plans, a risk assessment review and contingency options report. The last two deliverables are included as addendums to the plan (Devargas, 1999).

- Maintenance Program

In order for the continuity plan to reflect the ever-changing organisational needs, they have to be updated whenever necessary. Any change management procedures should be carried out in view of the developed recovery plan. The only deliverable for this phase is the business continuity plan (Devargas, 1999).

- Methodology observations
 - The methodology includes a component in the methodology that will help assess the health of the organisation with respect to information security. This component is the business health check report, one of the deliverables of the vulnerability assessment (Devargas, 1999). This report is the outcome of studying business areas such as backup and contingency planning procedures, insurance cover etc. The report could help to convince management and shareholders of the shortcomings of information security in the organisation.
 - The aim of the business impact analysis is to identify the critical business functions, determine the effect of their unavailability and calculate the possible financial repercussions as a result (Devargas, 1999). This methodology goes a step further by first identifying the business functions and then classifying them as critical, important or non-essential. This helps to simplify the prioritisation of functions.
 - As a final phase, this methodology includes a maintenance phase. The reason is that once developed, the continuity plan needs to be continually maintained. Most organisational changes will affect the existing continuity plan. By implementing change management procedures, as pointed out in this methodology, one can ensure that any changes will inevitably be reflected in the continuity plan (Devargas, 1999).
 - This methodology has a deficiency in establishing the importance of seeking management commitment. When a crisis or disaster strikes it could

have various effects on business. These effects could include losing important assets to the organisation, market position and business momentum. A business continuity plan must, therefore, be in place and be accepted by senior management as an insurance policy. Management has to understand the severity of the impact that disasters could have on the organisation. By doing this they indicate that they agree to provide the necessary labour and funding needed to complete the project successfully (Karakasidis, 1997).

- The majority of conventional BCP methodologies reviewed contains both a recovery strategy as well as a strategy implementation phase. The recovery strategies phase involves the development of different recovery options for various business functions (Devargas, 1999). The strategy implementation phase will include detailed procedures to restore business functions within the specified time frames for each (BS7799-1, 1999). This methodology unfortunately combines both as a single phase. These two activities are both very important and to emphasise this they should preferably not be combined.

3.5.2 Methodology 2

The IBM Business Continuity and Recovery Services Consulting Methodology consists of seven phases or components. These are: a risk analysis, business impact analysis, recovery capability assessment, recovery strategy, enterprise solution study, business continuity plan and IT recovery plan. Besides this, the entire methodology is further divided into three stages namely analysis, design and implementation (J. Roberson, personal communication, December 4, 2000).

- Risk Analysis

The purpose of the *risk analysis* phase is the identification of procedures that, if carried out, could possibly prevent or reduce the effect of a disaster. These procedures include educating personnel about issues such as security,

vandalism, workplace violence etc. A risk analysis exercise also involves the analysis of the organisational environment to identify threats that could lead to a disastrous situation. Areas to be reviewed for such threats are the actual physical location of the organisation, access security, the organisation's policies and practices and the construction of any of the organisation's facilities. The objective is to identify the vulnerabilities that could cause the most damage to the organisation and to select the appropriate controls for providing effective protection (J. Roberson, personal communication, December 4, 2000).

- Business Impact Analysis

The *business impact analysis* phase would involve the identification of the functions most critical to ensure business continuity as well as the time frame and required resources for each function. The reason for doing this is to develop an effective recovery strategy. This is done by reviewing these functions and prioritising them based on each function's recovery time frame. The Business Impact Analysis study has to gather information about vital records, systems control methods and the current recoverability of the organisation. Organisational procedures are also reviewed and if necessary, improvements are suggested (J. Roberson, personal communication, December 4, 2000).

- Recovery Strategy

The recovery strategy adopted by the current methodology is categorised according to the length of business function recovery windows. These categories are pre-stage, subscribe and acquire. The pre-stage category is used for recovery windows of minutes to a few hours.

It involves pre-planning for the critical resources that could include a fully operational and redundant data centre, carrying out the necessary critical operations or just switching incoming calls to a redundant call centre. The subscribe category is used for recovery windows of twenty-four hours to a

couple of days. During this time recovery service vendors are usually used to recover the data centre or workplace. The acquire category is used when the recovery window ranges from a couple of days to several weeks. The assumption made for this category is that all required resources would be purchased, rented or leased once the disaster has occurred (J. Roberson, personal communication, December 4, 2000).

- Enterprise Solutions Study

The *enterprise solutions study* phase entails implementing the solutions as developed during the recovery strategy phase. The critical functions are prioritised during the Business Impact Analysis phase and the developed plan will show the path followed to develop the required solution. The size of the projects at this stage is dependant on how much the current recovery capability differs from the desired recovery state. The plan timeframes will also depend on the difference between how much is spent on plan development and how much the organisation stands to lose if business continuity is affected (J. Roberson, personal communication, December 4, 2000).

- Business Continuity Plan

The *business continuity plan* phase entails the identification of tasks that need to be completed in order to support the recovery strategy and continuation of business functions. Activities include restoration of the home site, returning to the home site, insurance claim issues and dealing with liability issues. Certain recovery issues such as maintaining the plan, testing and exercising the plan, and recovery of business functions and data centre can even be outsourced if desired (J. Roberson, personal communication, December 4, 2000).

- IT Recovery Plan

The *IT recovery plan* phase contains all the tasks necessary to be completed in order to fully recover the data centre. These include activities usually forming part of a conventional disaster recovery plan such as the recovery of all systems and applications needed by the various business functions (J. Roberson, personal communication, December 4, 2000).

This phase also defines and implements the necessary tasks to fulfil the recovery strategy requirements. If the recovery strategy specifies a hot site for the data centre and a work site for a specific number of personnel, then the resources to make this possible must be acquired somehow. If a vendor will be used the vendor would need to provide for both these strategies to be implemented and still be competitive in terms of pricing and conditions. The vendor should also be able to provide for unique technology requirements (J. Roberson, personal communication, December 4, 2000).

- Methodology observations

- Most conventional continuity planning methodologies contain only a plan development phase or strategy implementation phase. The methodology in question also divides plan development into two separate sections. The first section concentrates on the development of a continuity plan. This section includes all those tasks involved with allowing business processes to continue without the services and facilities of the IT department. It also involves the recovery of these processes when necessary.

The second section, the IT recovery plan, refers to those procedures that are to be followed to ensure the successful recovery of the IT department (J. Roberson, personal communication, December 4, 2000). By separating the plan development into two individual sections, it is possible to complete each section independently. This would allow employees to concentrate

solely on continuity of processes in the one phase and exclusively on recovery in the following.

- This methodology lacks a project planning phase. The project planning or initiation phase usually includes all activities that need to be completed in order to initiate the BCP project (Heng, 1996). These include steps such as obtaining senior management support, defining the planning responsibilities, deciding on the project infrastructure, setting up schedules for interviews to assist with the BIA, etc. (Devargas, 1999).
- This methodology unfortunately does not include a testing phase. It is essential that business continuity plans are tested thoroughly to ensure that they are not flawed (BS7799-1, 1999). This would also allow employees and everyone involved in carrying out procedures stated in the plan how to react in the event of a disaster (Morwood, 1998). A separate testing phase is therefore required in the plan. During this phase testing objectives are established, the scope of the tests are determined and the results of the tests are evaluated (Smith & Sherwood, 1995).
- As with the previous methodology, a maintenance phase is omitted. Seeing that organisations are functioning in an ever-changing environment, a framework needs to exist with which to ensure that any changes in the organisation will be reflected in the plan. To ensure this, change management procedures must be incorporated into the methodology (Smith & Sherwood, 1995). This can best be done by adding a maintenance phase.

3.5.3 Methodology 3

The following methodology is described in an article entitled “*Developing a suitable business continuity planning methodology*” by Heng and was developed for the Standard Chartered Bank of London. The methodology was completed after several conventional frameworks and methodologies had already been reviewed and adapted to suit the bank’s environment (Heng, 1996).

- Project planning

The most important step in the *project planning* phase is to obtain senior management commitment. The fact that senior management acknowledges and accepts the BCP project is imperative to ensure success. Pre-project planning, which serves as preparation for the planning phase, should also be done. These activities would typically include the negotiations with relevant parties to ensure the availability of the required resources. It would also include combining collected planning information and appointing a manager to oversee the BCP project (Heng, 1996).

- Business Impact Analysis (BIA)

According to the methodology the BIA phase can further be divided into three steps. These are performing the BIA, determining the minimum processing requirements as well as analysing the risk. The final steps, namely analysing the risks, differ from the traditional risk analysis because it actually refers to the prioritisation of resources as well as the identification of possible loss situations for resources. Heng states that it should be stressed that business managers should be held accountable as soon as they are appointed. This is normally done once management has given their support for the project (1996).

- Recovery Strategy

During the *recovery strategy* phase the users are allowed to methodically analyse the recovery process without actually writing detailed recovery procedures. All the work completed in this phase allows users to visualise the organisation's approach to recovery and continuity. The phase also includes discussions with the appropriate authorities and the parties involved in the project before any effort is made to develop the necessary recovery procedures.

The *recovery strategy* phase includes the development of strategies for recovering the business functions and IT department, backup procedures,

identifying the minimum processing required and determining alternatives for processing recovery (Heng, 1996).

- Plan development

The Standard Chartered Bank makes use of continuity planning software to assist with the development of the business continuity plan. An important consideration during this phase is training users on how to use the software. The templates that form part of the software also need to be customised before any of the plans are created using the software. The plan includes stages such as emergency response, business and report functions recovery planning, the recovery process and returning home (Heng, 1996).

- Testing

Having reviewed various different methodologies, it has been noted that most other methodologies tend to combine the testing, training and maintenance phases to produce a single phase. The bank has, however, decided in their methodology that the training should be conducted as part of the testing. They do not, however, combine the two activities into a single phase, because during the second cycle of testing each of these phases has its specific purpose (Heng, 1996).

- Methodology observations

- This methodology combines the *training* and *testing* phases (Heng, 1996). Business continuity testing is an excellent learning experience for those involved in the planning project. It saves time by not physically having a training phase prior to testing. It furthermore allows better understanding of all recovery procedures by physically carrying them out during an exercise.
- Most of the methodologies reviewed have only a *plan development* phase followed by *testing* and *maintenance* phases. This would tend to indicate that after the plan development phase the plan is complete. It is, however,

not the case as the *testing* and *maintenance* phases are still to follow. Before testing has been completed, the plan is still flawed and needs to be updated based on the evaluated test results. Only once tested, the continuity plan can be seen as complete since all or most flaws would have been removed. The addition of an extra step to the methodology after the testing phase, as in this methodology, would indicate a state of completion. This shows the point in the methodology where the plan is completed to the point where it is maintained.

3.5.4 Methodology 4

The final methodology was developed by the National Institute of Standards and Technology (NIST). NIST is responsible for computer systems technology in the United States Federal government. Their goal is to develop standards and guidelines, provide technical assistance and to research computer and telecommunications systems to effectively utilise Federal information technology resources. The methodology consists of six phases. These are identifying the mission critical functions, identifying the supporting resources, anticipating disasters, selecting contingency planning strategies, implementing contingency strategies and testing and revising strategies (Guttman & Roback, 1995).

- Identifying mission or business critical functions

Ensuring the continuity of business processes can prove difficult if they are not clearly identified. It is essential that managers understand the organisation from a viewpoint that is wider than what they are used to. A business plan, which is the definition of the critical functions of an organisation, needs to be developed. This plan not only identifies the functions but prioritises them as well. It could happen that in the event of a disaster certain procedures will not need to be carried out. If the priorities for each business function have been set and have been approved by management it could play an important role in determining whether the organisation will survive a disaster (Guttman & Roback, 1995).

- Identifying resources supporting critical functions

Once the mission critical functions have been identified, the resources supporting these functions should be identified along with their usage timeframes. The effect that unavailability of these resources would have on the function should be determined as well. Identifying the resources is, however, not an easy task. Departmental managers regard some resources as important and could overlook others. Those individuals who understand how functions are performed should therefore analyse resources and interdependencies. This would simplify the prioritisation of identified resources (Guttman & Roback, 1995).

- Anticipating contingencies

Identifying all possible events that could affect the normal day-to-day functioning of the organisation could prove difficult. By doing this the organisation can use the developed scenarios to develop a plan that will cater for a wide range of disasters. The developed scenarios should include both small and large disaster situations. They should also include all the resources as identified in the previous step (Guttman & Roback, 1995).

- Selecting Contingency Strategies

Once the various scenarios have been developed, it is time to start planning for the recovery of required resources. When considering the alternatives one needs to take into account the controls that are in place in order to prevent or lessen the effect of disasters. Seeing that no collection of controls can prevent all possible disasters in a cost effective manner, the necessity exists to coordinate the prevention and recovery efforts (Guttman & Roback, 1995).

Recovery strategies usually consist of three activities namely emergency response, recovery and resumption. Emergency response refers to those activities that are performed immediately after a disaster to protect lives and

limit the damage caused by the disaster. The recovery step refers to the actions taken to ensure continued support for the critical business functions.

Resumption involves the return to normal day-to-day functioning (Guttman & Roback, 1995).

- **Implementing Contingency Strategies**

As soon as the development of the recovery strategies have been completed, it is time to implement these strategies, document them thoroughly and the train employees (Guttman & Roback, 1995):

- **Implementation** : Much preparation is needed when wanting to implement the developed strategies. One needs to, for example, set up procedures for backup as well as contracts and agreements. It would be necessary to negotiate existing contracts to make way for new services. This preparation would also involve assigning personnel to various tasks should disaster strike. The team to perform these tasks is often called the emergency response team

- Documenting : The documenting step involves the actual writing of the plan. The plan also needs to be maintained after any changes occur in the organisation and its systems. It needs to be well written in case of the unavailability of critical personnel. Tasks should be simple and clearly stated in order for someone with minimal knowledge and experience to be able to perform them effectively. More than one copy of the plan should also exist and stored safely for redundancy purposes.

- Training : It is important that all employees involved in contingency planning should be well trained in performing their duties. As soon as new personnel join the organisation they also need to be made aware of their responsibility towards continued operations. They should also be trained in performing the tasks assigned to them. Existing employees must also practice their tasks on a periodic basis. The training portion of implementation especially provides the necessary practice that will ensure that employees react appropriately.

- Testing and revising

A contingency plan will undoubtedly contain flaws and should therefore be tested vigorously in order to identify and correct these flaws. The plan will also become outdated as the resources supporting the critical functions change. One or more individuals should be made responsible for keeping the plan current. Various types of testing exists including reviews, analysis and disaster simulations (Guttman & Roback, 1995).

A review simply involves testing the contingency plan regarding its accuracy. This would, for example, include checks to determine if employee listings are current and that tasks assigned to them are still the same (Guttman & Roback, 1995).

A plan analysis is usually done by an individual not directly involved in the development of the plan but still has a good working knowledge of the different business functions and the resources supporting them. The plan is analysed by mentally following procedures stated in it in order to identify mistakes in the logic thought processes of the developers. The entire plan can be analysed at once, or only part of it if desired (Guttman & Roback, 1995).

A disaster simulation is a valuable tool for identifying flaws in the plan, as well as assisting employees to practice for actual emergencies. These tests assist in providing important information for assuring business continuity. They are, however, expensive to conduct. A rule of thumb is that the more important a function is to the organisation, the more cost effective it is to perform these simulations (Guttman & Roback, 1995).

- Methodology observations
 - The *implementing contingency strategies* phase found here can be seen as the equivalent of the *plan development* phase found in other methodologies. As pointed out in some of the previously discussed methodologies, the presence of a *plan development* phase is more effective if not combined

with the *strategy development* phase. This allows plan developers to concentrate on each phase separately, and thereby developing more detailed strategies and a detailed recovery plan.

- The majority of methodologies reviewed include a BIA phase consisting of identification of critical business functions, determining the maximum amount downtime allowed and critical function prioritisation. Most of these methodologies do, however, neglect to include the resources that support these functions. The resources are just as important as the functions themselves and the critical functions need these resources to survive. It is therefore imperative that these resources are identified and included in the recovery strategies and plan development, as is done in this methodology.
- This methodology identifies the first two steps as the identification of critical business functions and the identification of the resources that support these functions (Guttman & Roback, 1995). The BIA phase as found in most other methodologies contain both these steps. These two steps do not warrant two separate phases seeing that they are fairly similar activities and can be incorporated into a single phase.
- The *anticipating potential contingencies or disasters* phase, although an essential step, does not necessarily warrant a separate methodology phase. Including this step as one of the steps in the recovery strategy development phase would therefore be a better option. If the organisation has a basic idea of what could go wrong, they should be able to devise better strategies for continuing business and recovering critical functions and the IT department.

3.6 Conclusion

This chapter discussed the use and importance of methodologies especially for BCP projects. The concept of a methodology was defined through examining various definitions and views. The characteristics of an effective methodology were reviewed as well in order to determine what to expect from a methodology. The importance of methodologies in the

field of BCP was also discussed. It was pointed out why a methodology is an essential component in the continuity planning process and what is to be expected from such a BCP methodology.

The chapter furthermore focussed on four known BCP methodologies, discussing them in detail and analysing them in terms of advantages and drawbacks. From this analysis the criteria for an improved methodology could be identified.

In general, seven methodology phases were prominent. These were project *planning*, *business impact analysis*, *continuity strategies*, *plan development*, *testing*, *training and maintenance*. Some of the important, and also innovative, issues to be included in such a methodology were also identified. These are amongst others seeking management commitment and dividing the plan development phase into two stages for IT recovery and business process recovery. Having completed this step, one can now see what an effective BCP methodology should look like and what steps it should generally include.

The following chapter will concentrate on the characteristics of small to medium sized organisations. These characteristics will be taken into account when a detailed BCP methodology is devised to ensure that it is effective for small to medium sized organisations as well.

Business Continuity Planning in Small to Medium Sized Organisations

4.1 Introduction

The previous chapter discussed the concept of methodologies, especially how they play a critical role in the process of Business Continuity Planning (BCP). It furthermore analysed and evaluated four existing BCP methodologies. From these evaluations a clear picture was formulated that highlighted which phases are essential as part of a continuity planning methodology. Additional components, present in the reviewed methodologies, were identified as well to assist in the process of continuity planning.

This chapter will concentrate on small to medium sized organisations, and how continuity planning can be different in these organisations. It will firstly discuss the criteria by which they are classified. It will also discuss how these organisations differ characteristically from their larger counterparts. Finally, these differences in characteristics will be highlighted to play a role in designing a BCP methodology that would be particularly effective for small to medium sized organisations.

4.2 Classification of small and medium sized organisations

The majority of the information relating to BCP usually discusses the development of continuity plans for large organisation, omitting how this process might differ in smaller organisations. These sources usually specify that each BCP activity is to be performed by a separate team i.e. a team is needed for the Business Impact Analysis, another for the Risk Analysis etc. The problem is that resources and staff are limited, especially when it comes to smaller companies. The BCP project is also a non-revenue producing project and does not qualify as a high priority project for organisations (Weems, 1999). The following subsections will discuss how small, medium and large organisations are distinguished

between, with the objective to determine whether this might have an influence, specifically on BCP methodologies.

4.2.1 Classification according to workforce size

There are various different sources, each having its own collection of figures by which it categorizes small and medium sized organisations. The various figures do not differ much and are largely dependant on factors such as the country where the organisation is located and the type of organisation or business. Types of business include manufacturing, construction, transport, storage and communications etc. In a country such as Japan, for example, an organisation having 300 employees is regarded as a small-scale enterprise while in other countries an organisation having the same amount of employees is regarded as medium sized (Bowler & Dawood, 1995).

Small and medium sized businesses usually belong to the category small business along with very small and micro enterprises. These businesses range from local grocery stores and restaurants to relatively large manufacturing operations (Megginson, 1994). A small business can be defined as “independently owned and operated, it is not dominant in its field, and does not engage in new and innovative practices” (Griffin, 1990, p.738).

As have been mentioned, various sources mention different criteria for differentiating between the various categories making up small business. Barrow mentions that a workforce of ten to forty employees constitutes a small organisation while having fifty to five hundred employees would mean that a business could be seen as medium sized. Any organisation with more than five hundred employees would be regarded as large, while those with less than ten could be seen as belonging to the very small category. Barrow further mentions that the term employees, as used here, refers only to those who receive a salary and therefore excludes the owner/manager and family members (Barrow, 1993, p. 5).

The above-mentioned numbers apply specifically to French organisations. It must be emphasized that they differ, sometimes quite extensively, from one country to the next. In small countries such as Denmark and Ireland, these figures are adjusted accordingly to reflect the size of the country.

Small organisations are those with less than forty-nine employees and medium sized organisations employ 50 to 199 people. For a business to be considered as large here, it would have to have more than 199 employees. This approach is only logical, as it would not make sense to use the same figures adopted by a country the size of the United States for countries the size of France. No organisation would have enough employees to qualify as large (Barrow, 1993).

In South Africa the picture is once again completely different. Figures appearing in the Business Blue-Book of South Africa (2001) differ substantially from those found in Barrow. The act states that small businesses are divided into four categories namely micro, very small, small and medium sized enterprises. Medium sized organisations would have a maximum of 100 or 200 employees (this depends on organisation type) and no less than 50 employees. Those organisations that do have less than 50 employees would constitute a small organisation or enterprise. The very small and micro enterprises have a maximum of 10 to 20 and 5 employees respectively (Business Blue-Book of South Africa, 2001).

Although the numbers that have been identified in the above paragraphs are not standard for all countries, it can be seen that there is a distinct difference between small medium and large organisations when workforce size is involved. Workforce size is, however, not the only classification method for organisational size as annual revenue and capital assets can also be used.

4.2.2 Classification according to annual revenue and capital assets

According to Megginson, besides using the number of employees forming the workforce of an organisation, one can also use the annual turnover or revenue to determine size (1994, p. 11). Bowler and Dawood add to this the amount invested by the organisation in capital assets. They specify that for an organisation to qualify as a small and medium sized enterprise, it would have to have a maximum annual turnover of R5,000,000 and capital assets worth R2,000,000. Once again, as the case was with the number of employees, the precise turnover amount differs from one source to the next and also varies between the different types of industries.

The Business Blue-Book of South Africa (2001) states the turnover can range from R4,000,000 to R50,000,000 for medium sized organisations. For smaller organisations this amount ranges from R 2,000,000 to a maximum of R25,000,000. It also states that the capital asset values are between R2,000,000 and R18,000,000 for medium sized enterprises and R1,000,000 to R4,500,000 for small enterprises. Those organisations with very high capital asset values are industries needing expensive equipment and machinery, such as mining and manufacturing.

As the case was with workforce size, it could be seen that there is once again no agreed upon standards for the annual revenue and capital assets for small medium and large organisations. There is, however, a significant difference and that is important to realise.

The two distinguishing factors discussed in this section pointed out that smaller organisations differ extensively from larger organisations. Therefore one could more than likely expect a small workforce and reduced annual revenue to have an effect on the BCP process within an organisation. The following section will examine further organisational characteristics to identify their possible effect on BCP.

4.3 Characteristics of smaller organisations that affect BCP

Small businesses have an important role to play in the economy of just about every country. In fact, the greater part of businesses falls into the category of small business. These smaller organisations have an effect on a wide variety of areas (Griffin, 1990). This section will discuss small business characteristics that further set SME's apart from their larger counterparts.

- **Financial performance** : It is a well-known fact that small and medium sized organisations in most countries far outnumber the amount of large organisations. These businesses, on average, also perform better financially than large organisations, this of course being proportional to size.
- **Responsiveness to market conditions** : In manufacturing operations, for example, smaller businesses could respond better to changing market conditions at a smaller cost than large businesses (Griffin, 1990). Despite this, small organisations in general, as mentioned in section 4.2.2, have a much smaller annual turnover than large corporations.
- **Innovation** : One of the characteristics of smaller organisations is that they have been on the forefront of innovative breakthroughs. Examples of this are the inventions of the personal computer, the copy machine, the instant photograph, etc. (Griffin, 1990). These small organisations appear to promote individual resourcefulness due to a less restrictive environment (Barrow, 1993). SME employees' area of expertise is furthermore wide ranging (Johnson, 2002)

- **Communication** : In small organisations, communication systems are less formalised. Organisational communication is simple and information is more freely available. The ease of communicating is mostly due to the fact that there is such a small number of employees. Communication therefore takes place more efficiently and effectively (Johnson, 2002).
- **Job Creation** Barrow mentions that SME's, especially small organisations, are a major source of job creation. (1993, p 32). Not only this, but the rate of job creation in smaller organisations is also much higher than in larger organisations (Griffin, 1990).
Barrow (1993, p.33) indicates that smaller businesses across all sectors show rapid growth compared to larger businesses, especially with respect to workforce size.
- **Contributions to larger organisations** : Besides being fast growing and a major source of innovation and job creation, the majority of SME's also contribute to large businesses. Most of the suppliers to large businesses are smaller organisations and the reason for this is that these businesses can create and deliver specialised products and services more effectively than any of the large organisations providing an identical service. SME's are also key players in product distribution and selling for larger organisations (Griffin, 1990).

- SME environments : Given the physical size compared to large organisations, along with their limited resources, SME's are very much dependent on the state of the market. Changes in economic conditions force them to change as well. Larger organisations are not so much affected by these market changes and can go without change until it is absolutely necessary (Barrow, 1993). Smaller organisations can therefore be seen as operating in more dynamic environments than larger firms.

- Management structure : Besides for a greater number of employees and a larger annual turnover, larger organisations also have a larger management base than smaller companies. These organisations have a variety of different managers. Smaller organisations could for example not employ a risk manager due to various reasons, of which cost is certainly the most obvious. These smaller companies have a much smaller management team consisting of only the most essential candidates (Devargas, 1999, p. 35).
In small organisations managers are usually directly involved in the day-to-day activities and are also closer to their employees. This usually creates a more pleasant environment (Johnson, 2002)

- Infrastructure complexity : In general, the size of an organisation, in most cases, directly impacts the costs for these organisations, especially when recovery strategies are involved. Hardware and software for smaller organisations tend to be less costly than for large organisations. The telecommunications infrastructure also tends to be less complex and the volume of data supported by this infrastructure tends to be low as well (Beckmeyer, 2001).

- SME budgetary issues : Even though management is generally aware of the importance of BCP, they are reluctant to set aside a large budget for this purpose. The tendency for organisations is to set aside approximately 2 percent of IT budgets spent on BCP (Jackson & Carey, 1997). Unfortunately SME's do not have a large budget in general (Weems, 2000). When this is taken into account, it could be assumed that the IT budget, and the BCP budget, will be rather limited for SME's.

- SME conduct : Small organisations are generally less formal in the way operations are conducted. This usually leads to a more casual control environment. Personal example and verbal communication may be utilised instead, rather than formal instruction manuals used in large corporations. In these large organisations there is usually some proper code of conduct, which fails to create a culture of integrity and ethical behaviour (Johnson, 2002).

- Business mortality rate : Smaller businesses, in general, have a relatively high rate of failure compared to their larger counterparts (Carleton, 2002).

- Lack of in-house IT knowledge : In general, smaller organisations lack the required in-house IT knowledge that is essential for their survival. IT Consultants are, however, relatively expensive (Besoft, 2003). In larger organisations this tends not to be the case.

In the above sub-sections characteristics of smaller organisations were identified and it was shown how these characteristics set them apart from large companies. Along with the distinguishing factors identified in section 4.2, these characteristics will most likely have an affect on BCP within these smaller organisations. The next section will examine the effects of some of these characteristics on BCP.

4.4 Business Continuity Planning: A small business perspective

A few years ago the majority of organisations did not feel that BCP was important enough to devote company resources and personnel to, seeing that it is a non-revenue raising project. Today, however, this is no longer true. Whether an organisation is large or small, they still need to ensure availability of their IT infrastructure and services. This section will therefore discuss a variety of BCP related factors that are affected by the differences between small and large organisations, as examined in the above section. This section will attempt to indicate how a methodology needs to differ in order to prove effective for SME's.

4.4.1 Financial and budgetary BCP repercussions

The reason why BCP process is such a difficult one is that plans are drawn up to react to an event that has not yet happened. To ensure that the business continuity plan is effective in almost any type of situation, it must be flexible and must be easy to implement at any location, especially the alternate site. It is important to identify alternate processing strategies that are in line with the organisation's size and budget (DeLuca, 1996). It has also been mentioned in section 4.2.2 that smaller organisations' annual income is a lot less than for larger organisations.

Although these small organisations generally spend a great deal less on hardware and software, and have a much simpler telecommunications infrastructure, they still need to select a solution that suits their size and budget (Beckmeyer, 2001).

Weems, (1999) suggests that, once having identified the most appropriate alternate processing solutions, one should first ascertain which of these solutions management is not willing to fund. The other, more cost effective options therefore have to be considered (Weems, 1999). Therefore, in the case of SME's, a methodology should not include the more expensive solutions.

A further concern involves an organisation's backup strategies. It is not only important to regularly backup an organisation's data, but to store this data securely offsite (Gulley, 1999).

Various solutions are available to ensure secure offsite data transfer and reliable data recovery. Some of the more common options are regular tape backup and shipping, electronic vaulting and mirroring. The type of solution depends on how soon following a disaster will the data need to be available again. Electronic vaulting is unfortunately very expensive compared to regular tape backup. Mirroring involves duplication of data on an identical system and is also a very expensive and resource intensive solution (Hurwicz, 2000). Given an SME's limited budget and annual income, it is easy to assume that the last two solutions may not be cost effective. It is therefore suggested that a methodology catering for smaller organisations is mostly based on a tape backup and manual shipping solution for offsite data transfer.

4.4.2 Staff size and innovative effects

It has been pointed out in the above section that SME's do have a limited staff and also support innovative practises. This means that in smaller organisations employees can usually perform a wide variety of tasks (Johnson, 2002). One area where a limited staff size is bound to affect the BCP process is during recovery team identification. The number of employees in an organisation will always be a deciding factor according to Edwards (1994).

Recovery teams are commonly used on which to base the structure of the business continuity plan. These teams each have their own recovery responsibilities to ensure that the organisation operates as usual in the shortest amount of time (Wold & Vick, 2000). Team members should generally include members from a variety of departments. The size of the teams will, however, vary according to the size of the organisation (Dolten, 1996). Dolten (1996) further suggests that teams for smaller organisations should consist of one to two members only. The larger organisations can consider teams ranging from five to seven members. Another factor that might affect teams and members is employee innovation. Edwards (1994) mentions that it is a probability that specialist employees may have to serve on more than one team.

It has, however, been pointed out in section 4.3 that in smaller organisations, employees are generally not specialized and are able to perform a variety of tasks. This theory supports the concept of small teams for SME's.

It could be assumed, taking the above-mentioned into account, that even though teams will consist of one to two members, these teams' areas of expertise will be wide ranging. Small organisational teams will not need to be that large in order to complete their designated tasks due to an abundance of expertise within each team. A methodology for small organisations, therefore, needs to allow for the creation of an adequate amount of small recovery teams.

Another area that will undoubtedly be affected by a limited number of employees is appointing individuals responsible for overseeing the BCP project. Karakasidis (1997) suggests the selection of an entire BCP committee consisting of nominated recovery team managers as well as a senior recovery management team member. Such a team usually oversees the recovery process. Chances are, however, given the limited staff situation and the minimal number of teams, that an entire BCP committee is impractical. One could therefore assume, given the size of the organisation and the lack of staff, that an individual, perhaps the owner or manager, might prove sufficient to oversee the BCP project.

4.4.3 Job creation and SME environments

Most organisations operate in rapidly changing environments that include the addition, alteration and termination of business processes, the hiring or promotion of employees etc. (Moore, 1997). In section 4.3 it was mentioned that SME's environments are even more dynamic than those of larger organisations. The rate of job creation for SME's is much higher and they are changing rapidly, especially with respect to workforce size. According to Weems (1999) such changes in workforce size is one of the events that prompt frequent business continuity plan reviews and updates. From this, it could be deduced that such a high rate of change would require a high plan review frequency in smaller organisations.

The probability is relatively high that business continuity plans for small organisations need to be reviewed and updated more frequently than those for larger organisations. Generally, plan reviews and updates are conducted by means of either a fixed review schedule or by events that trigger the need for these updates, such as changes in personnel, processes etc.

These trigger events ensure that any organisational changes are reflected in the continuity plan (Weems. 1999). Seeing that small organisations tend to change more often, it could be deduced that a scheme that would involve all or the majority of organisational employees be utilised. Such a scheme would aim at ensuring plan dynamism by instantaneously reacting to these trigger events.

4.4.4 The effects of SME conduct and management structure

Obtaining management commitment prior to commencing the BCP project is crucial to ensure the success of the project. According to Johnson (1998) the following steps need to be completed in order to fully obtain management commitment:

- Request a policy statement
- Present the business case to sponsors
- Obtain formal project approval
- Issue recommendations after each phase
- Work within the budget cycle

The above steps will be discussed in more detail in the next chapter. Many of these steps, however, seem to indicate a very formal approach to obtaining management commitment. One such a step is *obtain formal project approval* and, according to Johnson (1998) includes steps such as writing a project proposal, specifying the cost and staffing requirements for the project etc. As section 4.3 indicated, SME's operate in very casual or informal control environments. It could, therefore, be assumed that formal project proposals are not often utilised in these smaller organisations.

Furthermore, management, as mentioned, is also smaller and their closer relationship with employees provides for better communication. Management in these organisations is more available to employees (Johnson, 2002). It is assumed, given their relationship, that employees would not need to make use of formal means, but rather communicate directly with management. Therefore, it can be suggested that most of the above mentioned steps could possibly be omitted. The first step is, however, an essential one seeing that management still needs some way to indicate their commitment and accountability (Smith & Sherwood, 1995).

A further effect of an informal operating environment is that management is so much more involved in the day to day running of the business. They are more aware of what their business requires to ensure success. Managements of larger firms are not that involved and, therefore, not as knowledgeable as their small business counterparts (Johnson, 2002). Making employees and management aware of the importance of BCP is essential. It is suggested that web pages, e-mail and intranet systems are used and even that time is set aside to educate employees on the importance of BCP (Crimando & Steinburg, 1997).

A number of small organisations do have a continuity plan in place and, therefore, are aware of the importance of BCP (Barclay, 2002). Once again, given the staff size and the relationship between staff and management, such drastic measures might not be entirely necessary. It should after all be easier for managers to communicate the importance of BCP to their employees or vice versa in such an informal environment.

According to the United States General Accounting Office (1998), a master schedule needs to be set up for the project along with the identification of milestones to be completed. Such a schedule will indicate delivery date for various project components (United States General Accounting Office, 1998). This approach resembles a very formalised and well-planned approach, similar to that described earlier in this section, when obtaining management commitment was discussed. Given the informal small business environment, it could be assumed that such steps would typically not be completed. Small business infrastructure, as

pointed out in section 4.3, is not as complex as in large organisations and requires simpler plans. Therefore, it could also be deduced that less planning would be required for the recovery of smaller organisations, making these above-mentioned scheduling and planning steps somewhat redundant.

One of the important steps when addressing the continuity strategies for the organisation is planning for a Public Relations (PR) exercise, should disaster strike. Huff (1998) suggests that a team consisting of a senior official, a public relations directors, legal advisors, finance representatives, technical experts etc. should be appointed. Given the management structure and limited staff of SME's, they will most likely not employ legal advisors, a human resources director etc. Just as with recovery team identification, it could be assumed that a PR team would most likely be small as well. Huff (1998) does after all mention that a PR team must be customized to suit the organisation. It is therefore suggested that an individual be made responsible for this instead on an entire team. Huff (1998) states that employees with the most technical and business knowledge might be most suited.

4.4.5 The effects of dealing with larger organisations

It is relatively common for smaller organisations to try and obtain some form of quality certification, such as ISO 9000, in order to deal with larger organisations (Davenport, 1995). Such standards ensure, through processes and procedures, that an organisation is competitive and can perform as expected. Furthermore, the quality management process figures well into the BCP process. The first reason is that both quality management and BCP require management commitment to provide the required assistance and resources for the project. Secondly, both these processes require frequent audits and reviews. With quality management it is to ensure that all products conform to norms and standards as set by the quality certification. With BCP, the same is done to ensure that the continuity plan stays continually updated (Baruch & Baruch, 2000).

Quality management thirdly requires that critical systems are backed up to ensure the integrity of the organisation. The same applies for BCP where regular backups are essential to ensure business continuity. Further similarities include the necessity

for a clear understanding of each employee's responsibilities within the organisation and good internal communication. Lastly, both BCP and quality management require continuous testing and training (Baruch & Baruch, 2000).

Therefore, the effect of smaller organisations' quest to be suppliers to large firms forces them to implement a business continuity plan and thereby ensuring continuity and availability of their services. According to Devargas (1999) it could lead to legal action if an organisation is unable to supply agreed upon products or services.

4.4.6 The effects of organisational infrastructure

In larger organisations the IT infrastructure is much more complex than in smaller organisations. The size of the business does, however, not determine whether a business continuity plan is necessary. Rather, the criticality of the IT services and business functions are the determining factors. Beckmeyer argues that, in some circumstances, the process of BCP could be even more important and advantageous for small businesses than for larger companies (Beckmeyer, 2001).

A further factor to keep in mind is that organisations, even if their size is not taken into account, are all different. In some companies the IT infrastructure may be represented by a standalone computer. For this company, a backup plan that ensures the regular backup of data, and that the data is taken offsite and stored, should be adequate (Beckmeyer, 2001). A full business continuity plan, containing recovery procedures, continuity procedures etc., would most likely be redundant. In a medium sized company with a more complex infrastructure, such as a LAN and a collection of workstations and servers, a business impact analysis may be utilised to identify suitable recovery strategies, specifying that a disaster recovery plan is enough (Beckmeyer, 2001).

If the above-discussed holds true, it is logical to assume other scenarios may exist, where smaller organisations will require the above, along with a collection of contingency plans or even a full business continuity plan, catering for backups, disaster recovery, business continuity and other BCP related options. All the

previously mentioned options are methodology implementation issues seeing that only selected BCP steps have been chosen for implementation.

It is therefore suggested that an implementation method for BCP methodologies must cater for situations where organisations do not require a full business continuity plan, but rather certain parts thereof.

In the above sub-sections it could be seen that the BCP process might differ in a variety of ways in small to medium sized and large organisations. These differences can mainly be attributed to the characteristics of SME's, as discussed in section 4.3, that distinguish them from large organisations.

4.5 Conclusion

Material discussing the development of a BCP methodology for small to medium sized organisations is not in abundance. For this reason, this chapter studied the characteristics and methods for classification of organisational size. It was found that two criteria, namely the workforce size and annual revenue, were mainly used for classification. SME characteristics were identified and discussed to determine how these smaller organisations differ from large firms. Finally, these characteristics were studied in line with BCP requirements to determine how BCP would differ for smaller organisations. It was seen that existing, detailed BCP methodologies had to be altered in some cases to cater for the specific needs of SME's.

The next chapter will concentrate on the development of a complete and detailed BCP methodology. All the necessary criteria were identified and discussed in the preceding chapters. In section 4.5 it was determined that similar BCP methodologies could be used for small and large organisations, but they should at least be scalable to simplify implementation for SME's. The next chapter will, therefore, discuss the various required phases and the detailed steps to be performed in each for producing an effective business continuity plan for small to large organisations.

A Detailed Business Continuity Planning Methodology

5.1 Introduction

In the previous chapter it was concluded that the methodology used for implementing Business Continuity Planning (BCP) in smaller organisations might differ from those used in larger organisations. The reason for this is that Small to Medium Enterprises (SME's) have less resources available than larger organisations and also have in some instances, different focuses. A large number of BCP methodologies do exist, but when studied it becomes clear that they are more suited to large organisations. One reason for this is that sources concentrating on the development of a BCP methodology for small to medium sized organisations are not easily found. Characteristics of smaller companies and methods for size classification were furthermore discussed. Finally, the chapter concluded by identifying some factors and characteristics that might have a specific influence on the methodology and/or the implementation thereof in small to medium sized organisations. These were financial performance, responsiveness to market conditions, innovation, communication, job creation, contributions to larger organisations, SME environments, management structure, infrastructure complexity, SME budgetary issues and SME conduct.

Chapter 3 described a methodology as a logical sequence of steps designed to efficiently guide us to the successful conclusion of a project. It would, therefore, be unwise to dilute a good complete BCP methodology to simplify the BCP process for SME's. A better idea would be to make sure that the suggested BCP methodology for SME's, while kept complete, is made scalable to ensure that it could be implemented even with limited resources. The implementation method utilised must also be adapted to cater for SME's and their restrictions with regard to large organisations.

This chapter will discuss in detail a methodology based largely on the different methodologies studied in chapter 3. The proposed seven phase methodology will take the

influencing factors and characteristics of small to medium sized organisations into account. These factors were discussed in chapter 4 and were based on the characteristics that distinguished SME's from their larger counterparts with regard to BCP.

Each phase will point out what needs to be accomplished during that specific phase. This will be done mainly to show what a reasonably complete and effective methodology should look like. It will contain the most important aspects that need to be present in a BCP methodology to produce an effective plan to be used in SME's. When completed, this methodology will be scalable, to cater for small and large organisations, depending on their specific needs and available resources, in this regard.

5.2 The Project Planning Phase

The project planning phase incorporates all those activities required to ensure that the BCP project is properly planned. Of these activities, securing executive management support is probably the most important to ensure project success (Heng, 1996). Further important elements include a high-level awareness campaign to educate employees and top management, establishing a BCP workgroup, holding a BCP orientation meeting and determining the project prospects.

5.2.1 Ensure top management commitment

Since a disaster or disruption in business could have a serious effect on the organisation, it has to be brought to management's attention what the possible effects would be if a disaster does strike. They will have to accept the notion of a business continuity plan and commit themselves entirely to the project before any BCP related activities are performed. They must understand the reason for and approve all decisions made. Furthermore, they must commit to the provision of the necessary funding and labour needed throughout the continuity planning process. It must also be ensured that they lend their support to the testing and maintenance of the business continuity plan once completed (Karakasidis, 1997).

To guarantee the above-mentioned, there are various steps that need to be taken (Johnson, 1998):

- Request a policy statement : To formalise their commitment to the BCP project, senior management must issue a policy statement binding them to the project.
- Present the business case to sponsors : Along with top management commitment, it is also a good rule of thumb to ensure project sponsor commitment. These so called sponsors primarily refer to those individuals in middle management with whose support the project will be much more credible. A solid business case should be sufficient to convince them.
- Obtain formal project approval : The next step is to obtain formal approval for the BCP project. The way to go about this is to prepare a project proposal that includes important cost estimates and staffing requirements. This proposal should furthermore be distributed and signed by the managers of those areas that are affected to indicate their approval.
- Issue recommendations after each phase : To increase project manageability, it helps to divide the project into phases. A benefit provided by such an approach is the ability to obtain management approval incrementally. Once each phase is completed it is possible to issue recommendations on how to proceed with subsequent phases. Also, the completion of a phase demonstrates the ability to produce results.

This in turn will give management some comfort, making it easier for them to commit.

- **Work within the budget cycle** : A project can easily be affected by budgetary irregularities. The BCP project has to be reflected in the departmental budgets for management to approve overall requested expenditures. The individual responsible for BCP has to approach the various departments during the annual budgeting process to ensure that BCP elements are considered.

The key organisational SME characteristic that would play a role here is SME conduct. The previous chapter did mention that the above-discussed steps, or the majority of them, might in most cases be seen as being redundant for smaller organisations. This is mainly due to the fact that small organisational operational environments are less formal and, therefore, these more formal procedures may prove to be unsuitable.

5.2.2 Conducting a high level awareness exercise

As soon as the required policies have been produced, they need to be brought to the rest of the organisation's attention. Setting aside some time to educate personnel allows for the distribution of the necessary BCP information. All measures taken by the organisation to ensure safety and to communicate during a disaster situation should also be conveyed to the employees. To increase awareness even further, the organisation can make use of Web sites, group e-mail and intranet systems. Employees can then learn more about disaster recovery in general or specific aspects of it when they have time. They could even access this information from home after hours or if they are unable to get to work in case of an actual disaster (Crimando & Steinberg, 1997).

These informative websites should contain examples of disasters, how they affected other organisations and how these disasters were dealt with. They also form a

useful tool for making employees aware of how disasters can affect them personally. For this purpose, an organisation should publish their BCP related policies. These policies will assist in making employees aware of what is expected of them with respect to BCP. For example, employees might want to know more about salary payment methods during disaster situations. Finally, websites should include other BCP links for those who are interested (Turley, 2000).

During this step, management structure and size are bound to play a role, as pointed out in the previous chapter. In SME's, given that management is normally more knowledgeable with regard to the operational issues than in larger organisations, and given the physical size of the organisation, it would mean that a formal awareness exercise might not be necessary. If such an exercise is, however, undertaken, the communication characteristic can be seen to play a role. Information distribution, and especially BCP related information, normally occurs much simpler in SME's and any BCP information should, therefore, be easy to distribute during an awareness exercise.

5.2.3 Establish a business continuity planning committee

As soon as management commitment has been achieved, and employees along with management have been exposed to the concept and importance of continuity planning, it is time to appoint a BCP committee or individual to oversee the project. A project manager must consequently be appointed. Such a committee must include recovery team managers and preferably senior management representatives as well (Karakasidis, 1997). In the case of smaller organisations, appointing an individual instead of an entire committee should be sufficient.

This committee or individual is responsible for approving the members chosen for the various recovery teams. Further responsibilities include supervising the creation of awareness documentation, planned and unscheduled tests, the appraisal of employees' and management's level of awareness (Karakasidis, 1997). The organisational size characteristic would definitely influence this step seeing that an organisation could most likely not spare too many employees for this purpose.

Furthermore, the selection of an entire committee might be construed as too formal, which means that SME conduct plays a role as well.

5.2.4 Determine project prospects

Determining project prospects involves the identification of milestones and the setting up of a master schedule for the entire BCP project. The schedule needs to indicate the estimated delivery dates for the various project components. Furthermore, targets or objectives that need to be completed must be identified if realistic completion dates are to be determined (United States General Accounting Office, 1998).

This is once again seeing that SME conduct would most likely play a role with respect to this step. The previous chapter pointed out that, given the informal small business environment, it could be assumed that the above steps would typically not be completed. Small business infrastructure is not as complex as in large organisations and requires simpler plans. Due to less planning to ensure recovery of smaller organisations, the above-mentioned scheduling and planning steps could more than likely be omitted.

All the above-mentioned steps are essential to ensure that the BCP project is well planned. Therefore, whether an organisation is large or small, they cannot afford to neglect any of these steps. Smaller organisations simply need to complete them in a way that suits them. The planning committee identification step is an example of this. Here, smaller businesses will simply identify an individual instead of an entire committee. In the above sections, SME conduct, organisational size, management structure and communication were found to influence the project planning for the BCP project. Once planned properly, the BCP process will concentrate on identifying critical business processes and related factors. This will be discussed in the following section.

5.3 The Business Impact Analysis Phase

As planning for the BCP project has now been completed, the next logical step is to identify and then analyse the business processes that are critical to the organisation. This is done through a Business Impact Analysis (BIA). The aim is to separate those processes without which the organisation cannot function as usual from those that are less important or even redundant. An analysis of each process should include the identification of all costs emanating from the inability to complete the process, because of some disaster or event, as well as the resources required by each (Wilson, 2000).

After the analysis of processes, they are generally prioritised by means of a predetermined ranking system. The maximum amount of time each can be unavailable before business is impacted is also determined during the BIA. Once this has been done it is possible to understand the impact that various disasters may have on business (Gordon, 2000) The rest of this section will, therefore, discuss the process of performing the BIA. Specific steps will include the identification of critical business processes, identifying various disaster scenarios, determining the various costs involved, prioritising the critical processes and determining which resources are critical to each process. It must be indicated that none of the steps discussed below have been found to be directly influenced by the identified SME characteristics.

5.3.1 Identifying critical business processes

To identify the mission critical functions, one has to take all business units and areas into account. Every department or business unit must list all vital functions that form part of the daily operations for that department. The best way to accomplish this is to physically record the daily activities within each department. A period of two weeks to a month should be sufficient to analyse the functioning of each department. During this period it should be possible to identify all the vital functions both internal and external to each department (Wold, 1996). There is no perfect method for reviewing an organisation's business processes. All possibilities will inevitably have risks, scope problems and time constraints associated with them (Fisher, 1996).

Fisher (1996) firstly suggests making contact with various senior executives and asking them to identify those departments they see as critical to their operation. They then select the personnel they feel should be included in the analysis sample. Continuity planners should make sure that they record all the vital information pertaining to the descriptions of the business processes. These are the size of each process, the main purpose the process is intended for and the critical activities performed by each. The size of each process refers to, amongst others, the total revenue generated, the total number of employees involved, the number of customers affected by each process (Wold, 1996).

5.3.2 Identifying failure scenarios

Identifying all the possible disasters or events that could affect an organisation is a physical impossibility. Continuity planners must, however, still strive to identify most of these scenarios that could be cause for invoking the business continuity plan or part of it. These scenarios could assist an organisation to develop a continuity plan applicable to a wide range of events. These scenarios should address both small and large contingencies and planners should use both research and imagination to identify the less obvious scenarios (Guttman & Roback, 1995).

As an example, a business process involving delivering stock to various clients will be considered. The planner then needs to consider scenarios where firstly, only part of the process cannot be performed and also where the entire process cannot be performed. By using these scenarios, an organisation can later determine how severe the effect of unavailability might be (Nosworthy, 1999). According to Guttman & Roback the developed scenarios should consider the various resources required for each process such as human resources, processing capability, automated applications and data, computer-based services, infrastructure, and documents and papers (1995, p.123):

- Human resources : Scenarios should include situations where employees are unable to travel to work. It should further be determined whether essential skills and knowledge are limited to one individual only. Furthermore, it should be determined whether the alternate site is accessible to everyone.
- Processing capability : Scenarios where the computer equipment is damaged or destroyed completely should be considered. Furthermore, scenarios should include situations where only part of the equipment is unusable.
- Automated applications and data : Scenarios should be considered where data integrity has been compromised or where sabotage played a role. Furthermore, the possibility for applications to run on other platforms should be considered.
- Computer-based services : Scenarios where computer-to-computer communication is no longer available should be considered. Partial availability of the communications network should also be considered. Further scenarios should include the communication difficulties between employees and the status of information services.
- Infrastructure : Scenarios should include situations where employees cannot occupy the building for a certain amount of time. Not having the necessary equipment for performing their daily tasks must also be considered as a possibility.

- Documents and papers : Scenarios must consider the situation where required documents and papers cannot be found. If they can be found, scenarios should cater for the possibility that they are unreadable.

5.3.3 Calculate criticality factors

Various factors need to be considered in order to determine the importance of, and later prioritise, all critical business processes. These are the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) and the costs associated with the impact on business processes.

5.3.3.1 Determining the Recovery Time and Point Objectives

The Recovery Time Objective (RTO) refers to the maximum amount of time a process or system can be unavailable for. If the RTO is large, the less it will cost an organisation. In other words, the longer the RTO, the larger the costs incurred due to the unavailability of the process (LaPedis, 2001). Each business process needs to be examined and assigned an RTO. To accomplish this, both managers and staff involved in each process need to agree on this assigned value. The length of the RTO depends largely on how keen employees are to find alternatives for continuing each process (Button, 1995). A further factor that needs to be identified for processes is the Recovery Point Objective (RPO).

RPO is a factor indicating how current a specific data set is and needs to be determined for all data. This value needs to be identified if a suitable backup method is to be chosen. If the data should not be more than four hours old, for example, before the disaster occurred, one should choose the appropriate backup method or technique (Gordon, 2000).

Only using the RTO and RPO as prioritisation values are however not sufficient. Though some business processes might not need to recover as quickly as others, it does not mean that they are not critical. Therefore, the cost of the impact on each business process needs to be taken into consideration as well as to determine

the criticality factor of each process (Button, 1995). Therefore, the next sub-section will identify the various costs that need to be identified for prioritisation purposes.

5.3.3.2 Determining the costs of impact

This sub-section will discuss the costs that are incurred as the result of a disaster striking. The aim is to identify these costs and use them to produce a ranking value, which will then be used along with the RTO to prioritise the critical business processes.

The three types of costs that need to be identified are tangible, intangible and operational costs (Button, 1995):

- **Tangible costs** : These costs usually refer to values that can be determined easily by valuing the items they apply to. Examples of tangible costs include lost revenue, labour hours and impending penalties or fines (Wilson, 2000). As these values are easily calculated, they are usually also covered by insurance.
- **Intangible costs** : Intangible costs normally include those costs of which the exact values cannot be determined. The costs in question are affected by any negative influences on the organisation's reputation that have been gained with time. Examples of these costs are the loss of credibility, a decline in the level of customer service and all other activities that could negatively influence how the organisation is perceived (Wilson, 2000). Even though it is difficult to identify the exact monetary value it is important to know how these costs will affect each business process.

- **Operational costs** : Operational costs are those costs that are undertaken to ensure that a business process can continue while the IT department is recovering. They would, for example, include acquiring additional equipment and personnel to cope with the processing requirements during a disaster situation.

5.3.4 Prioritising business processes

As have been previously mentioned, the time tolerance of each function is not enough to determine the recovery order for organisational processes. Therefore, values have to be established for costs that have an impact on business processes. Seeing that tangible and operational costs could be identified easily, the following table could be used to determine each one's impact value (Button, 1995):

Description	Value
Very Low Impact	1
Noticeable Impact	2
Significant Impact	3
Severe Impact	4
Very High Impact	5
Critical Impact	6

Table 5.1: Tangible and Operational Cost Values

The reason why no monetary values are used in this table is that monetary impact values for large organisations obviously differ from smaller organisations. That is why the impact value is only qualitative (Button, 1995).

It is difficult to assign a value to intangible costs. For this reason, a table with impact ranking is once again used to identify the intangible cost for each business process. The scale of one to six is used again to keep the method for determining impact costs standard. The following table could therefore be used (Button, 1995):

High	-----	Medium	-----	Low
6	5	4	3	2

Table 5.2: Intangible Cost Values

Once values for tangible, operational as well as intangible costs have been identified, an average value, which represents the total cost of impact, needs to be calculated.

This value is simply the average of the three combined impact costs, i.e. the sum of these three cost values as determined using the appropriate tables, divided by three. This average will later be used along with the RTO to determine process priorities (Button, 1995). Finally, the RTO value for each process needs to be identified. For this purpose, another table is used to determine a ranking for each business function (Button, 1995):

Time Period	Value
0 to 6 hours	1
6+ to 48 hours	2
2 to 5 days	3
5 days to 2 weeks	4
2 weeks to 2 months	5
2 months to 2 months +	6

Table 5.3: RTO Values

The two identified values, the average cost and RTO values, can now be used to determine process priority by plotting each process on the Time Tolerance and Cost of Impact graph, as defined by Button (1995) and depicted in figure 5.1. When all identified business processes have been incorporated into the graph, their position on the graph can be used to determine their various priorities. The graph is divided into sectors ranging from 1 to 6.

The most critical processes are those found in sector 6 and the least important processes are found in sector 1 on the graph. Therefore, processes should be recovered starting from sector 6 (Button, 1995). Having conducted this exercise, a priority value will have been identified for each business process.

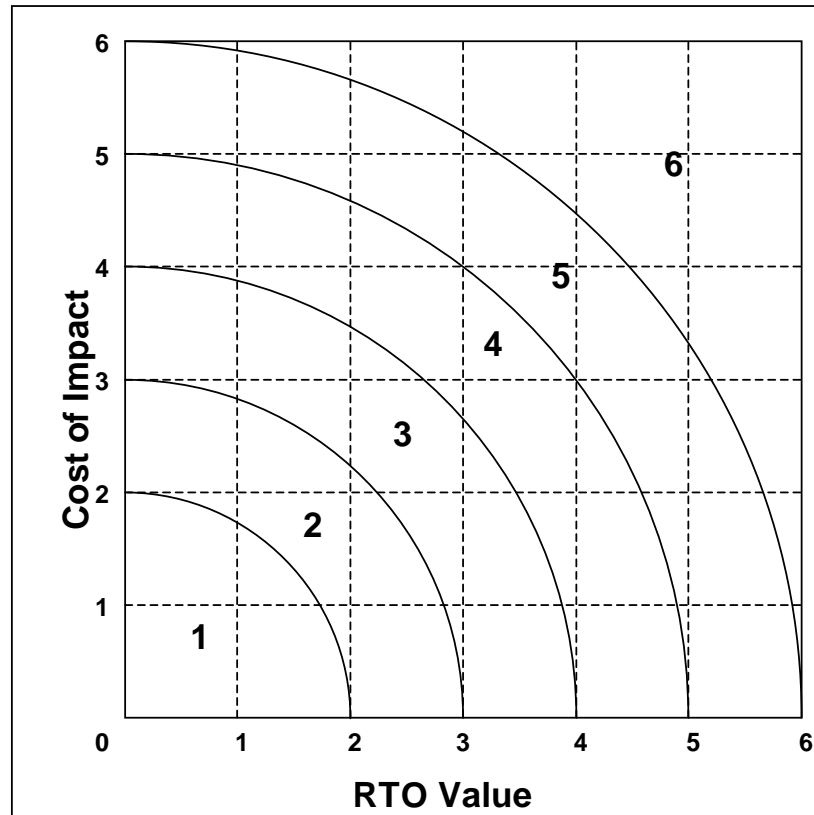


Figure 5.1: Time Tolerance and Cost of Impact graph

5.3.5 Identifying supporting resources

After having identified the organisation's business functions and ranked them according to cost and time tolerance, one has to identify the resources that support these functions. The usage time frames of these resources and the effect of their unavailability must furthermore also be identified. They are not necessarily computer resources. They include everything required to perform each function. Only those that have a working knowledge of a business process should engage in resource identification activities. Resources should also be prioritised and those

resources that are essential to each process must be identified (Guttman & Roback, 1995).

Resources that need to be identified include employees, equipment, applications and data, computer-based services, infrastructure, and documents and papers (Guttman & Roback, 1995). Gordon (2000) suggests various techniques for accomplishing this. Firstly, specialised equipment and their usage should be identified along with the impact of prolonged unavailability. Furthermore, the ability of the process to function without access to online databases should be examined. Any special forms and other supplies that are needed to perform each function should be listed.

Communications equipment is another factor that plays a role in the continuance of each function. The dependence on communications, therefore, also needs to be identified for each process. Further concerns, amongst others, are staff members that are cross trained to perform a variety of tasks, applications and databases used by each process and all application dependencies (Gordon, 2000).

To conserve resources during the business impact analysis, smaller organisations could make use of questionnaires along with interviews or a small decision making group. Furthermore, employees could be interviewed in groups or interviews could include only those employees that would supply critical information. Seeing that the Business Impact Analysis is largely an information gathering exercise, these suggestions could help smaller organisations to conserve valuable resources (Weems, 1999).

Once all the above Business Impact Analysis steps have been completed, an organisation should have a clear understanding of which processes would have the greatest impact if unavailable, a listing of potential disaster scenarios for each process and what essential resources are required for each process. The above-mentioned information contributes to the selection of cost effective recovery and continuity strategies for the business. The selection of these strategies will be discussed in the following section.

5.4 The Business Continuity Strategies Phase

This phase entails the identification of various strategies that focus on ensuring business continuity and recovery. It requires the reviewing of the various identified disaster scenarios to develop methods to deal with these situations. Continuity and recovery strategies can be as simple as identifying backup procedures for the storage and retrieval of critical data. Certain strategies may be more suited to some scenarios than others because of the type and severity of a disaster (Wilson, 2000).

An organisation should, therefore, preferably have more than one continuity strategy developed, one for each process. The strategies for one process will of course inevitably overlap with the strategies for some of the other processes. They should only aim to provide the minimum acceptable requirements for ensuring continuous operations. (Nosworthy, 1999). This section will, therefore, concentrate on the various tasks to be completed to develop effective strategies. These are identifying the appropriate backup strategies, IT recovery strategies, business continuity strategies, insurance options, user holding strategies, working with the media and emergency resources.

5.4.1 Identifying backup strategies

Ensuring continuity of business processes and the recovery of the IT department are almost physically impossible without data. Therefore, if an activity has to be chosen as a first step towards a recovery plan, it is the backing up and protection of an organisation's critical data (Koski, 2001).

5.4.1.1 Backing up data

An organisation should take steps to ensure that procedures are in place to ensure the continuous availability of their data. Software should, therefore, be backup up frequently and stored at a secure offsite location (Romney, 2000). Not only should they ensure the backing up of computerised data, but they should protect critical documents such as deeds, contracts, personnel files, tax records etc. as well (Moore, 1995, p. 26-27). Various steps need to be performed to ensure that information can be successfully recovered (Goggins, 1999):

- Firstly, all an organisation's vital information must be identified along with its storage location. Data to be backed up includes system software (operating

system files, start-up files and operational files), application software (program suites, start-up files and operational files) and corporate data (user files, databases etc.) (Tydlaska, 1996). User files will typically include the critical data on end users' hard disks as well (Takemura & Taylor, 1996). Other locations for data include servers, laptops, palmtops, RAID systems and the hard disks of those employees who telecommute (Koski, 2001).

- Secondly, a backup method must be identified. Two well know methods are file and image backup. With file backup each file is requested individually and written to the backup media. Image backup copies an entire disk onto the backup media. File backup provides accuracy while image backup provides speed of recovery (Koski, 2001)
- A good backup plan should thirdly generally include procedures that specify the backup frequency of identified data. Such a plan should furthermore specify who will be performing these backups and where they will be stored (Tydlaska, 1996).
- A fourth consideration is the amount of copies that are to be stored of the backed up data. More than one copy should also exist, preferably three according to industry standards (Tydlaska, 1996).
- A fifth consideration is that the data should be easily obtainable in event of an emergency and it should be specified who is authorised to retrieve the backups. Furthermore, the time it will take to retrieve the data must also be determined (Goggins, 1999).
- Lastly, the amount of time it will take to restore the backups must be determined and the person(s) responsible for data restoration must be identified (Goggins, 1999).

5.4.1.2 Transporting data offsite

Once all data is backup up, it needs to be securely stored for swift recovery during disaster situations. Typically, an offsite location needs to be far enough away not to be affected by the disaster as well. An increase in distance does, however, increase transportation costs (Larue, 2000). Transportation of backed up data can be carried out physically or electronically.

When physical methods are used, the organisation is responsible for delivering the data to the offsite location themselves, or they could make use of overnight carriers. The drawback of overnight carriers is that it can become less cost effective as the amount of tapes to be delivered increases. An organisation could also make use of an offsite storage vendor. In this case the vendor is responsible for managing the backup transports and archiving.

The drawback of this approach is that it could be very expensive for smaller organisations. Organisations can, however, be certain that backups are handled professionally if they use this approach (Gulley, 1999).

Data can also be transmitted electronically to the offsite location by means of electronic vaulting. Depending on the type of connection used, this approach could be very costly. A dedicated line would ensure swift backup and recovery of data, but could prove expensive. Another option is sharing a connection or making use of a smaller line. Unfortunately the drawback then is the data transfer speed and the recovery time (Gulley, 1999).

If the continuous availability of an organisation's data is of utmost importance they can also consider mirroring the data on an identical system. Therefore, organisations must evaluate the recovery windows and how critical the data is when choosing an approach (Hurwicz, 2000). Financial performance and SME budgetary issues are bound to play a role when it comes to choosing an appropriate backup strategy. Chapter 4, therefore, suggested that for smaller organisations tape backup might be the most cost effective option seeing that the other available options might prove too expensive.

5.4.2 Identifying processing alternatives

In the case of serious natural disasters such as fires or floods, it may be necessary that an organisation will have to exchange their current premises for an alternate location (Hawkins, Yen & Chou, 2000). A business continuity plan must always cater for this possibility in case of a worst-case scenario. For data processing operations, choosing an alternate site approach could be a complicated task. The issues that need to be considered when choosing an alternate site are mainly the costs involved and the organisation's tolerance for downtime. If business will not be affected by the loss of data processing services for at least a week, having a fully mirrored site is completely unnecessary (Ginn, 1989).

The following are the some of the most common recovery alternatives available (Hawkins et al., 2000):

- Vendor maintenance agreement : This approach utilises the services of computer hardware vendors and they are then responsible for replacing, repairing and recovering hardware. For those organisations with relatively small networks, this is an effective approach. A standard agreement might not cover all possible expenses such as fire or flood damage. A supplemental agreement may then be necessary.
- Quick shipping program : This approach involves a contract requesting the delivery of hardware to the main or alternate processing site within three to five days. Maintenance costs are also kept low. Organisations that can afford network downtime of a week or more should consider this agreement.
- Hot site : Hot sites are fully equipped sites and furnished

according to the organisation's requirements. It also features living facilities such as lodgings, showers and a cafeteria. Hot sites are ideal for practising the continuity plan without disrupting normal business operations. Hot sites are generally maintained by a disaster recovery plan vendor.

- Cold site : A cold site is a building that houses no equipment, but is ready to accommodate any equipment at a word's notice. It is fully wired and air-conditioned This approach is only an option if the recovery time is relatively long because equipment needs to be set up and configured first.
- Warm site : Warm sites refer to a location or alternate site that is only partially equipped with the necessary hardware, network interfaces, power sources etc. to ensure recovery (Salemo, 1999).
- Mobile recovery facility : Implementing this approach requires a self-contained mobile trailer housing the necessary equipment. These trailers usually have backup power generators installed. Typically, the recovery time when using this approach is a week or longer.
- Mirrored site : This approach is very similar to the hot site option and is equipped with all the necessary equipment and communications facilities. The only difference is that it is company owned and data is transmitted regularly to this site. With this approach, an organisation can usually be up and running within a day.

- **Reciprocal agreement** : The reciprocal agreement involves identifying another organisation with similar requirements and facilities for temporary usage during a disaster situation (Romney, 2000). This is a cost effective approach. However, problems could arise with hardware and software compatibility if one of the parties changes their configuration (Guttman & Roback, 1995).

Financial and budgetary issues will more than likely influence the selection of an alternate processing strategy. In chapter 4 it was suggested that smaller organisations firstly must evaluate identified alternate site options before the most cost effective one is chosen. Therefore, due to their limited resources, smaller organisations must eliminate those options that management are not willing to fund.

5.4.3 Identifying user holding strategies

The user holding strategies are those strategies that detail the responsibilities of employees while the business is still functioning normally. The aim is to identify the tasks that can be performed while the organisation is functioning normally to ensure business continuity at a later stage. Examples of responsibilities include printing out reports that will be helpful in a disaster situation when IT services are not available. Part of this strategy is to determine which reports would be required and whether these reports should be printed out on a monthly, weekly or daily basis (Button, 1995).

5.4.4 Insurance coverage review

Chances are that any organisation that sets out to develop a business continuity plan will spend a large amount of money and time on the project. Without funding to implement it, the plan is of no value to the organisation.

Most organisations will of course have some insurance coverage but the question is that of adequacy. Organisations have to realise that insurance policies need to be reviewed constantly to reflect their ever-changing environment. There is no

standard insurance solution when it comes to insurance. An organisation should take a worst-case scenario as an example. They should ask themselves what would happen if the business site were completely destroyed and what it would cost to start doing business again. Consider difference in price between new and used equipment (Rospond, 1996).

The first coverage that should probably be considered is business income insurance. This type of coverage protects against a loss in net profit resulting from a disaster. It further covers continuing expenses such as rent and loan payments that an organisation has to continue paying despite the disaster situation. This coverage, therefore, assists the organisation to recover quicker and retain their existing customers (Van Mill & Gliane, 1997).

A further coverage that can be considered is extra expense coverage. It covers all expenses incurred besides the normal operational expenses. Examples of such expenses could be hot site fees, transportation and hotel costs, cellular phone purchases etc. Another consideration for coverage is ordinary payroll. Therefore, with this coverage an organisation would not have to be concerned about not having funding to pay employee salaries. Besides all of the above-mentioned considerations, organisations will of course have to ensure that they are covered for basic property damage caused by fires, floods etc. (Van Mill & Gliane, 1997).

Finally, to determine the amount that the organisation wants to be insured for, Paradine suggests one of two methods (1995). The one method makes use of the amount that the organisation would expect to earn for the duration of the interruption along with the operating costs incurred. The sum of these identified amounts will then form the amount to insure for and should ensure that the organisation is adequately covered.

A second method involves taking the turnover that is typically expected during the indemnity period and then subtracting all those items that the organisation do not want to insure. The difference is then the value the organisation will be insured for (Paradine, 1995).

5.4.5 Public relations

Organisations often neglect to appoint one or more individuals responsible for communicating the status of the organisation to the media and the community following a disaster or event. Two important issues that have to be covered are internal and external public relations.

It is just as vital to keep employees and the community up to date on the recovery efforts in order for them to feel comfortable with the situation. Employees would, for example, want to know that they would still be compensated for their services regardless of the circumstances. The chosen spokesperson will be given the task of relaying all this information to the relevant parties (Moore, 1995, p. 25-26).

The chosen spokesperson will also need to gather information from various parties. Therefore, various individuals need to contribute to the public relations exercise. Huff states that a very important part of establishing strategies for public relations is that of building a crisis communications team (1998). Choosing the right team will guarantee that public confidence is kept at a high. If at all possible, the team chosen should preferably include employees performing the following functions (Huff, 1998):

- Public relations (PR) management function : This is one of the most important functions in the crisis communications team whether the organisation is large or small. A PR manager has the authority to make decisions that could affect the public image of the organisation. They would also most likely make the initial statement after a disaster has occurred.
- PR directorial function : Once the initial disaster statement has been made, the appointed PR director will take over. Relationships and credibility with the media should already be established at this point and this makes

the PR directors well suited for this task. Although it is the PR director's duty to represent the organisation, support from the rest of the team is essential.

- Management of operations function : There is always the possibility that the disaster could affect one or more of the business processes. The operations manager would possess the necessary information to assist teams in the PR process.
- Legal advisory function : Any decisions made by the crisis communications team may have legal consequences. It would, therefore, be advantageous to have access to an attorney purely for advice and not to make any decisions in the PR process.
- Human resources directorial function : When it comes to issues such as timely employee communications and notifying the next of kin, someone having experience with human relations will deal with it better. The human factor is an important consideration in crisis communications. The HR director will, therefore, take care of more personal matters.
- Finance function : When a major disaster strikes, organisations will inevitably need emergency funds. A finance representative could ensure the availability and proper allocation of funds. This could include hotel and travel costs, communications equipment costs etc. and the financial representative is responsible for making funds available.

- Technical expert : One should never underestimate the media's function knowledge of technical issues within industry. It could be very helpful after a disaster to understand the reason for the event occurring. It could, therefore, be helpful to have technical experts to explain all technical issues involved. Sometimes, these experts could even speak directly to the media to explain certain complicated issues or simply give the PR director advice.

It is not necessary to build a team consisting of each of the above suggestions, but a team should rather be tailor made to suit a specific organisation and the organisation industry (Huff, 1998). As stated in the previous chapter, appointing an individual to be responsible for public relations should prove sufficient. For this reason it can be seen that staff size will affect the selection of a public relations team. Furthermore, SME conduct might also play a role as they, as shown in chapter 4, will not usually appoint formal committees, but rather an individual for such tasks.

The various different strategies as discussed above all contribute, either directly or indirectly, to IT infrastructure recovery and business continuity. Some steps focussed solely on backup and recovery of information and the systems that utilise and store this information. Other steps focussed on ensuring business continuity. A further collection of steps, such as public relations, insurance coverage and user holding strategies, could not be categorized as recovery or continuity activities. Rather, they could be said to contribute to BCP as a whole. The characteristics found to influence the Business Continuity Strategies phase were financial performance, budgetary issues and SME conduct. The next step would involve business continuity plan creation and this will be discussed in the following section.

5.5 Continuity Strategy Implementation

For each of the strategies defined in the previous section, detailed functional plans must now be developed with which to respond to the various scenarios. In order to produce detailed and effective plans, this task should be entrusted to those with the technical and business knowledge to accomplish this (Smith & Sherwood, 1995, p.19). The only Strategy Implementation step found to be influenced by SME characteristics is the selection of recovery teams. The various sub-sections that will be addressed are; emergency response procedures, process continuity and recovery procedures and finally establishing a continuity plan team structure and tasks.

5.5.1 Identifying emergency response procedures

To successfully respond to a disaster, detailed procedures need to be developed, given to personnel and preferably tested before any disaster occurs. It is imperative that an organisation responds as well as it possibly can in the aftermath of a disaster. This will ensure that their employees are protected along with the organisational assets and will help alleviate the disaster recovery process in general (Nosworthy, 1999).

5.5.1.1 Emergency notification procedures

There are various considerations that need to be taken into account when deciding on the notification procedures for a business continuity plan. Issues to be taken into consideration are those who need to be contacted, how they will be reached, will normal communication be possible, who will contact them, the notification list update frequency, where the copies of the list will be stored and the communications equipment that need to be made available (Moore, 1995, p. 23).

5.5.1.2 Plan invocation procedures

When deciding on how to respond to a disaster, in other words when to activate the business continuity plan, it is always important to consider the nature of the disaster. Depending on the seriousness of the incident the plan should contain

different courses of action for each level of disruption. It would, therefore, be a good idea to pre-establish different levels upon which will then be acted appropriately (Frost, 1994).

Frost uses as an example, three conditions namely green, amber and red. Depending on the condition, different courses of action should be taken (1994, p. 14). It should, therefore, be ensured that the plan is written in such a way that only the parts that will deal with the incident will be invoked (Ginn, 1989).

5.5.2 Writing process continuity and recovery procedures

The second step in implementing continuity strategies is the development of procedures for both the business processes and the IT department, or data centre as it is better known (Campbell et al., n.d.). These procedures should be simple and easy to understand so that anyone would be able to follow and complete them (Guttman & Roback, 1995).

5.5.2.1 Process continuity procedures

The process continuity procedures are those methods with which employees could continue the critical business processes, manually or otherwise, for the RTO period determined for each during the BIA. This is not a high priority to employees and this makes the task of writing the procedures difficult (Campbell et al., n.d.). LaPedis (2001) suggests that the most effective way of writing continuity procedures is to allow the employees involved in each function to complete this task. This approach has various advantages. In the first place, the procedures will be accurately written as the employees perform them every day. Secondly, time will be saved as various functions can write their plans simultaneously and lastly, employees feel that they have a stake in the creation of the continuity plan. The only task that the continuity planner will have is to be available for advice during the writing of the continuity procedures.

5.5.2.2 IT recovery procedures

Writing the recovery procedures for rebuilding the IT department is best done by making a checklist of the recovery activities. The employees that will carry out each activity need to be identified, along with personnel that will act as a backup for each employee. Tasks that need to be completed to rebuild the operating software, databases and the data up to before the disaster or incident must be identified (Campbell et al., n.d.).

5.5.3 Establish continuity planning team structure

The next logical step in implementing the various strategies will be the definition of teams responsible for carrying out the continuity procedures. According to Edwards (1994) the size of the organisation will inevitably have a role to play in the selection of the number of teams. It is advised that an organisation should consider a large number of small teams rather than a small number of teams each having a large number of responsibilities.

The teams identified could include any of the following:

Management, emergency response, damage assessment, security, notification, facilities support, administrative support, logistics support, user support, departmental recovery, computer backup, offsite storage, systems software, communications recovery, applications support, database recovery, production, computer restoration, internet restoration, human relations, public relations, purchasing and transportation, legal recovery, risk management, accounting recovery, financial support and travel support teams (Wold & Vick, 2000).

Having all the above-mentioned teams will of course be impractical in a small organisation. The organisational size, needs and complexity will be used to identify the needed teams. Most organisations, however, make use of the following four teams or a combination thereof (Wold & Vick, 2000). As mentioned in chapter 4, small organisations will typically make use of recovery teams consisting of a maximum of two members.

5.5.3.1 The management recovery team

This recovery team frequently includes a business continuity administrator and a business continuity coordinator. The administrator usually has the task of supervising the recovery project and providing assistance to team leaders. Final decision making usually rests with the administrator. The coordinator is responsible for coordinating activities between the various teams. Further responsibilities could include plan development and maintenance, plan distribution, continuity training and plan testing (Wold & Vick, 2000).

The general team responsibilities include receiving the initial disaster alert, verifying and determining the severity of the situation, deciding when to activate the continuity plan, notifying all the relevant parties, coordinating all activities of the recovery process and establishing the emergency operations centre. Further responsibilities include provision for equipment and supplies at the necessary facilities, documenting all recovery activities, reporting on the status of the recovery project and also continuously monitoring the recovery process (Wold & Vick, 2000).

5.5.3.2 The administrative recovery team

The responsibilities of the administrative recovery team may include activities such as taking care of insurance issues, all payroll activities, public relations activities, issuing press releases if required, ensuring that transportation progresses smoothly, ensuring adequate security for all operations, liaison with police and fire services, the selection of temporary personnel if required and organising security at all facilities (Wold & Vick, 2000).

The administrative recovery team may want to prepare a press release template for possible disaster situations. Information that should typically be included should be the amount and type of damage, the immediate status of the organisation following the disaster, instructions to organisational employees,

instructions to the community and reassurance that the crisis will be handled (Wold & Vick, 2000).

5.5.3.3 The user recovery team

The responsibilities of the user recovery team will include amongst others the notification of key employees, important vendors and other parties that have to be made aware of the immediate activities to be completed, verifying the status of employees after a disaster, identifying methods for performing high priority activities, keeping the departmental staff up to date, ensuring that required support services for operations are available and supervising the user departments' recovery process (Wold & Vick, 2000).

5.5.3.4 The technical recovery team

The overall responsibility of the technical recovery team is the restoration of systems that have failed from both a technical and operational perspective. They will, therefore, have the following responsibilities with respect to technical recovery of systems:

Setting up a help desk, restoring the communications network, restoring the required computer equipment, restoring applications to a usable state, restoring backups of critical files and databases, providing staff where necessary to supervise operations, the acquisition and setting up of additional hardware and other equipment, performing all file backups, retrieving the required backups stored offsite, activating the alternate site if necessary and deactivating the alternate site when the organisation is ready to return to normal operations (Wold & Vick, 2000).

The characteristics that could affect the selection and size of recovery teams are staff size and innovative effects. Chapter 4 explains that due to staff having a wide area of expertise, it is not necessary to have large teams. Due to limited staff, SME's also need to keep teams small.

All the above-mentioned strategy implementation steps also, like the Business Continuity Strategies steps, contribute to the recovery of IT services and continuity of business processes. These steps could be categorized as well by determining whether they support recovery or continuity. Completing all the above-described steps will result in a detailed business continuity plan. Next, employees need to be introduced to the plan through an awareness exercise. This will be discussed in the following section.

5.6 The Continuity Training Phase

Having a recovery team structure in place, with well-defined procedures, will ensure that team members will have guidelines available that tell them what needs to be completed by each team. To effectively perform these procedures though, they will need some training. The majority of organisations have part of their budget, resources and staff set aside for training in general. Business continuity training must also form part of this training framework and must be allocated part of the training budget. The training should be carried out as soon as the plan is complete as well as when it undergoes significant changes.

Furthermore, all new personnel should undergo training as well as those employees that gain new responsibilities by changing positions within the organisation (Morwood, 1998). This section will concentrate on business continuity training, more specifically awareness training. Awareness training can be divided into two categories namely introductory and detailed awareness training.

5.6.1 Introductory awareness training

The introductory awareness training session will be aimed at those staff members who will not participate directly in execution of the plan. Approximately an hour should be spent explaining the organisation's BCP methodology, the continuity strategies and the most important recovery and continuity procedures. Employees should especially be made aware of issues concerning organisational responsibilities, emergency evacuation procedures, recovery groups and their tasks, liaison with the media and emergency services and the major administrative support procedures. Morwood (1998, p. 29) further suggests that a similar exercise

should be conducted for senior management members who are not directly involved in the process. The session should however focus more on business issues.

5.6.2 Detailed awareness training

The detailed awareness training will be aimed at those employees who play a direct part in executing the continuity plan. More time will have to be spent on this session than the previous to discuss the continuity plan in detail. Morwood suggests approximately half a day. The information covered should be more or less the same than in the previous session, except in more detail. The specific responsibilities and tasks of employees must be clearly explained along with discussing how the recovery teams will support these activities (Morwood, 1998).

Once awareness training has been completed, employees at all levels of the organisation should be well informed about the importance of BCP for them and the organisation. Furthermore, those employees who play an active role in the BCP process should be well aware of their responsibilities and all questions they might have should have been answered. SME characteristics that would most likely play a role during this phase are staff size, communication and organisational conduct. Awareness exercises will, therefore, most likely be of an informal nature and because of a smaller number of employees, training groups will probably be small as well.

Next, there is a need to rehearse what needs to be done in a disaster situation, seeing that knowledge alone is not enough. Furthermore, it needs to be established whether the continuity plan is effective. The next section will, therefore, discuss BCP testing.

5.7 The Continuity Testing Phase

Once developed, business continuity plans must be tested to determine whether all the individual contingency plans are adequately written to ensure continuity of business processes and the recovery of the data centre. Furthermore, testing will help to determine whether the plans can be implemented in the required period of time (United States General Accounting Office, 1998). Testing has another distinct advantage, namely that it provides an excellent training opportunity for all personnel involved. It will show the

continuity planner which indicates that employees understand their responsibilities and can carry them out successfully (Karakasidis, 1997).

5.7.1 Developing test plans

Prior to conducting any tests to verify the validity of the continuity plan, an organisation must develop test plans. These plans must be approved by management before implementation. Once this step is completed, the plans should be distributed to the relevant personnel and advice given to those who may have questions.

The test plans should cover various issues such as the objectives of the tests, the equipment and other resources that are needed, all the personnel that need to participate in the tests, testing schedules that stipulate when and where tests will take place, the test procedures and the results that are expected (United States General Accounting Office, 1998).

Prior to testing, teams need to be briefed to explain issues such as the boundaries of the test as well as other technical uncertainties. Additional briefing sessions may be necessary to explain issues clearly if the test is a complex one. Topics that may need to be covered during these sessions are the test purpose, the objectives for the teams involved, the established disaster scenario, the time of the test, where teams will be located, the restrictions for each team, and the test assumptions (Edwards & Cooper, 1995).

5.7.2 Conducting the tests

Before it can be said with certainty that the business continuity plan is complete and will be effective in a disaster situation, it must undergo a series of rigorous tests. These tests can be hypothetical, component, module and full tests. An organisation does not necessarily have to perform each of the test types. The size and complexity of the data centre determines whether it is appropriate to conduct all the tests. If for some reason it is not possible to conduct a full test, as many modules tests as possible should be carried out (Edwards & Cooper, 1995).

5.7.2.1 Hypothetical tests

The purpose of hypothetical tests is to ascertain whether the required procedures are in fact present in the continuity plan and to determine whether they are theoretically correct. This test should preferably be carried out at least every six months. A worst-case scenario is defined and the entire plan is examined based on this scenario (Edwards & Cooper, 1995). Test participants are not expected to physically perform any activities. They must simply explain how they would handle various situations established within the scenario (Morwood, 1998, p. 30).

5.7.2.2 Component tests

A component is an instruction set specifying how a certain recovery procedure is performed and is the smallest section of a continuity plan. An example would be a process called “System Load” which involves all the procedures to load the system. The carrying out of these processes may however be completely different in a disaster situation. They may be carried out completely different depending on the situation. This must be tested completely to rule out the possibility of incompatibility problems (Morwood, 1998). The process of conducting component test may include, amongst others, the following activities (Ginn, 1989):

- Working through the recovery procedures of various components
- Testing whether the notification list for each component is correct
- Examining the offsite storage to ensure the presence of required data and resources
- Conducting an alternate site test (if applicable to the module)

5.7.2.3 Module tests

Module tests involve the testing of a few combined continuity plan components. All components should preferably have been tested before module tests are attempted. This type of testing aims to validate the recovery and continuity procedures when a group of components are tested simultaneously. The organisation can be confident that if they complete all module tests successfully that they will be able to survive a disaster even if they neglect to, or are unable to, carry out a full test. If no individual component tests are performed organisations usually find that unexpected problems surface (Morwood, 1998). The activities to be performed when conducting these types of tests are roughly similar to those of components tests.

Examples of module tests include (Morwood, 1998):

- Activating the alternate site
- Recovering all or some of the applications
- Recovering the communications network
- Recovering databases and systems

5.7.2.4 Full tests

The objective of a full test verifies that all components within all modules can be carried out within the identified time frames for each. The test furthermore attempts to verify that it is easy to progress from one module to the next without any problems. Full tests have two main objectives (Morwood, 1998):

- To ensure that the recovery can be carried out in the required time frame as indicated in the plan
- To test whether there is a smooth transition from one module to the next

The full test can also be conducted as a surprise disaster drill. This should, however, only be attempted when extensive component and module testing have been performed. To accomplish this only a few employees should be notified of the

test. Furthermore, a test date that does not greatly affect operations should be chosen. Funding for the test must also be addressed prior to testing (Ginn, 1989).

5.7.3 Analysing the test results

The testing process can only be finalised once the test results have been constructively analysed. This analysis maintains the momentum achieved through testing and this is a necessity in the plan creation process. Through regular involvement in testing activities staff also become more committed to business continuity. The analyses of test results consist of a debriefing session and creating a test report (Edwards & Cooper, 1995).

5.7.3.1 Conducting a debriefing session

The debriefing session should preferably be conducted by the business continuity planner. If an organisation does not have a dedicated continuity planner, this activity is performed by the management recovery team leader. The aim of the debriefing session is to make all parties aware of the results and other findings. These will make it easier to suggest improvements for the continuity plan at a later stage. Objectives that will be included in the test report can also be developed by reviewing these findings. Possible items for discussion could include the overall performance, the individual team performance, any other relevant observations, areas of concern and the type and estimated time for the next test (Edwards & Cooper, 1995).

5.7.3.2 Writing a test report

Once the test has started, all team leaders must maintain a log of events throughout the exercise. The information contained within these logs is used, along with the test manager's post-test report to produce a combined test report. All identified sections that need improving are handed to the relevant team leaders together with a realistic date to correct it. The test report could include, amongst others, the following sections (Edwards & Cooper, 1995):

- An executive summary of the test outcome
- A summary of the results of the test
- A summary of team performances
- A list of actions to complete before the next test

For smaller organisations it may be logical to assume that writing a test report, which is a more formal procedure, is an optional exercise. Report writing may therefore be only applicable to larger organisations.

BCP testing is essential to ensure that the produced business continuity plan is effective to allow business continuation and recovery in almost any type of disaster situation. Furthermore, these tests serve to ensure that employees are proficient in their BCP responsibilities. The SME characteristic most likely to play a role during this phase is SME conduct. Formal steps, such as writing a test report and conducting a formal debriefing session, could, therefore, more than likely be omitted.

Organisations do however change from time to time. When this happens, it must be determined whether these changes affect the existing continuity plan and whether it needs to be updated. The next section will therefore focus on business continuity plan maintenance.

5.8 The Continuity Plan Maintenance Phase

It is imperative that a business continuity plan is reviewed regularly and updated if required. This is done to ensure that the plan stays effective and up to date. Organisations should preferably have change management procedures in place to ensure that reviews and updates occur in a standard way.

One or more employees should be made responsible for managing the maintenance process. The continuity plan might need to be updated as the result of changes in various areas. These could include changes in personnel, contact details, legislation, the business strategy, vendors and customers, business processes etc. (BS7799-1, 1999).

A structure needs to be in place with which to ensure that any organisational changes will get reported to the appropriate individuals. If these changes then affect the current continuity plan it must be updated to reflect the changes.

The steps that need to be included in a change management methodology are reporting the changes, determining the impact of the change, updating the continuity plan and signing off on the changes (Button, 1995):

- Reporting changes : Any changes in the organisation need to be reported to a central point. The individual or individuals responsible for plan maintenance needs to record all reported changes.
- Determining change impacts : All the submitted changes need to be reviewed to determine whether they affect the continuity plan or not. If the continuity plan needs to change it is up to the appointed individuals to effect the changes.
- Updating the continuity plan : Once changes have been identified it is necessary for all team leaders involved to sign that they are aware of the change and indicate whether the change affects them. If this is the case, it is up to them to inform the rest of the team and update their section of the plan.
- Signing off on changes : Once the changes have been made to the plan, all the parties that have a stake in the development and implementation should be notified. All the teams must sign off on changes made. Once this is done, those in charge of change management must sign off as well as soon as they are convinced that the changes are correct.

Characteristics that might play a role during the maintenance phase are job creation, SME environments, SME conduct and responsiveness to changing market conditions. Both job creation and SME environments, as stated in chapter 4, create the need for continuous plan

maintenance. Responding to a changing market will probably have the same effect as the aforementioned. The above-mentioned maintenance steps could also be construed as very formal and therefore not entirely suited for the small business environment.

Once all maintenance steps, as described above, have been completed, one can more or less say that the BCP process is complete. Maintenance is, however, an ongoing process and the plan must continually reflect the organisation and any changes taking place.

5.9 Conclusion

This chapter introduced and discussed a detailed BCP methodology, which was based largely on a study of four existing and relatively recent methodologies. These methodologies were discussed in chapter 3 along with their various strong and weak points. These strong points were utilised and weak points addressed in designing this seven phase methodology.

Further factors that were taken into consideration during methodology design were small to medium sized organisational characteristics, as discussed in chapter 4. Most methodology phases were, therefore, made scalable, so that small and medium sized organisations could implement this methodology with limited resources available. The characteristics and the phases they influence are summarised in the table 5.3.

	Methodology Phases						
	1	2	3	4	5	6	7
Financial performance			•				
Staff size	•			•	•		
Responsiveness to market conditions							•
Innovation				•			
Communication	•				•		
Job Creation							•
Contributions to larger organisations							
SME environments							•
Management structure	•						
Infrastructure complexity							
SME budgetary issues			•				
SME conduct	•		•		•	•	•

Business mortality rate								
Lack of in-house IT knowledge								

Table 5.4: A summary of SME characteristic effects

Those areas that are greyed out in the above table could not be directly attributed to a single methodology phase. The contributions to larger organisations merely ensure that smaller organisations improve their service to large organisations by implementing a business continuity plan, the reason being that, as discussed in chapter 4, larger organisations often require their suppliers and general service providers to have such a plan in place. A less complex infrastructure in smaller organisations creates the need for an approach to simplify plan creation for these infrastructures. Such an approach will be further elaborated upon in the following chapter. Therefore, it does not directly affect any of the methodology phases. The same could be said for the last two greyed out areas, seeing that they do also not affect only a single or combination of phases, but rather BCP in general for an organisation.

Even though a complete methodology has now been developed, some problems concerning the implementation of the methodology still exist. Not many sources exist that specify how BCP methodologies should be implemented.

Furthermore, smaller organisations may choose not to implement the entire methodology because their infrastructure does not warrant a complete business continuity plan. Therefore, an implementation approach that could assist small to medium sized organisations in implementing a full BCP methodology, or only a section, could prove useful. Such an implementation approach will be discussed in the next chapter.

A Cyclic Approach to Business Continuity Planning

6.1 Introduction

Small to medium sized organisations differ in a number of factors from their large and corporate counterparts. This might have an influence on the successful implementation of a business continuity plan. For this reason the methodology of such a Business Continuity Planning (BCP) project should preferably be scalable to allow organisations with restricted resources to also enjoy the ‘insurance’ of a proper business continuity plan. These factors and how they might influence the implementation of BCP in small to medium sized organisations were discussed in the previous two chapters.

The above-mentioned methodology resulted from a study of various current methodologies to identify the common phases and innovative steps belonging to each. From this study seven phases were selected and incorporated into the above-mentioned methodology. These are the project planning, business impact analysis (BIA), business continuity strategies, continuity strategies implementation, continuity training, continuity testing and plan maintenance phases. An important factor that was taken into account in this seven phase methodology, was scalability.

As a detailed, scalable methodology has now been defined and discussed, implementation issues need to be considered. As the implementation of BCP methodologies is not a widely discussed subject, this chapter will propose and discuss an implementation approach. The approach will be aimed at simplifying the implementation of any BCP methodology, especially for smaller organisations with limited resources.

6.2 A cyclic implementation

The implementation of a BCP methodology through a cyclic approach will occur in four different stages, or cycles as they are referred to by this method. Each cycle has different disaster recovery and business continuity related goals. The approach is also not limited to specific methodologies, but should be applicable to most methodologies provided they are BCP related.

Many different BCP methodologies exist, but few of them provide any guidance or implementation alternatives. The cyclic implementation approach acts as a template that guides an organisation in partitioning an existing methodology and provides guidance for successful implementation. This section will, therefore, specify the purpose of each cycle with the aim of simplifying the process of deciding which steps should be performed during what cycle, with a specific objective in mind.

To explain the concept of a cyclic implementation approach an example will be used. The idea behind this approach could be compared to building an outer city wall as was done in medieval times. Building such a wall would obviously not be a simple task. If, for example, it was decided that the wall should be twenty feet high, building a twenty foot section along one part of the city at a time would offer no protection until the whole wall has been completed. However, if the wall were to be built in phases, it would provide some degree of protection whilst the project is still being completed.

During the first phase, the wall could be built five feet high around the city. This would, for example, serve to keep out small predators threatening the livestock. The next phase would involve continuing the building process until the wall is ten feet high. At this height, the wall would succeed in keeping out the small predators as well as protecting against threats which the five-foot wall did not cater for. Further improvements would include raising the wall to a height of fifteen feet and finally twenty feet. The twenty-foot wall will keep out the majority, if not all, of the anticipated threats. Each phase, therefore, builds on the previous by adding functionality to that which already existed. By utilizing the method described in the above example, one could divide a methodology into four separate cycles. Each cycle, as already mentioned, will concentrate on a different BCP related goal.

The cyclic approach is depicted in figure 6.1. The BCP methodology discussed in chapter 5 is used to illustrate the mechanisms of this approach. During each cycle all seven phases of the methodology are completed before the next cycle commences.

The essence of the individual phases from one cycle will, however, differ from those in other cycles, in terms of the number of methodology steps completed. In other words, the steps from the continuity strategies phase in the backup cycle will be different to those for the continuity strategies phase in the recovery, contingency and continuity cycles. The next section will discuss the goal of each cycle and will then apply the cyclic implementation approach to the previously discussed methodology.

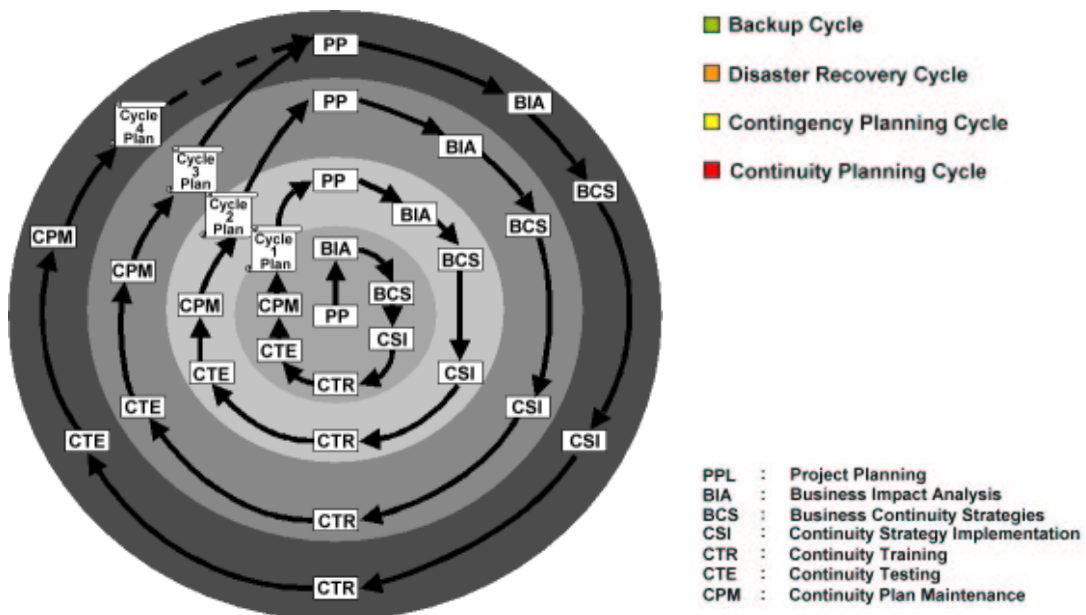


Figure 6.1: A cyclic approach to Business Continuity Planning

6.3 A discussion of the four BCP cycles

The complete methodology is divided into four distinct cycles, each with a specific objective but all on route to the final ultimate objective. The four cycles are the backup cycle, disaster recovery cycle, contingency planning cycle and continuity planning cycle.

The *backup cycle* concentrates mainly on ensuring that all organisational data is protected and readily available on request. This includes the regular backup of all data located

throughout the organisation. The backup process is not reserved exclusively for data in electronic format, but essential papers, documents and contracts as well. Furthermore, along with backing up of data, this cycle also involves dealing with the safe offsite storage of data along with determining which methods are best suited for transporting the data offsite.

The *disaster recovery cycle* involves primarily those activities related to restoring IT to its original, or close to original state. The main methodology phases that come into play are the continuity strategies and strategy implementation phases. Issues such as recovery alternatives, emergency response procedures and the recovery procedures are core methodology steps that form part of this cycle.

The *contingency planning cycle* aims to ensure the continuation of all the most critical business processes while IT partially or completely unavailable and recovering. Like the preceding cycle, the main methodology phases that play a role in reaching the goal for this cycle are again the continuity strategies and strategy implementation phases. The user holding strategies, or interim procedure options, as it is also known, along with writing the continuity procedures form the core steps for this cycle.

The final cycle, the *continuity planning cycle*, includes all those activities that ultimately complete the continuity planning process. Generally, these are the steps from the continuity strategies and strategy implementation phases that have not been completed yet as they attribute to accomplishing the preceding cycles' goals. They include, amongst other things, ensuring that insurance policies are sufficient to cover losses, the organisation is equipped to handle public relations, and emergency resources are readily available in case of disaster.

To illustrate the mechanics of the cyclic approach, the seven phase BCP methodology, discussed in the previous chapter, will be used as a sample methodology. The following sub-sections will discuss how this methodology has been partitioned to accommodate the cyclic approach.

6.3.1 The backup cycle

If an organisation has no access to their data after a disaster, it is virtually impossible to recover. Having an effective backup strategy in place lays the foundation for further recovery efforts (Koski, 2001). For this reason the backup cycle has been chosen as the point of departure for implementing a BCP methodology. Though the backing up of organisational information is at the heart of this cycle, all activities belonging to this cycle are not all backup related. All other methodology steps applicable to the backup cycle will therefore be discussed in the following sub-sections.

6.3.1.1 The Project Planning phase

As this is the first cycle, it is essential that all BCP planning activities are incorporated. Project planning steps such as securing management commitment, holding a high-level awareness exercise, establishing a BCP workgroup and determining the project prospects need to be present. Senior management support needs to be obtained for the entire project at this stage and not just for the current cycle. It is probably the first time management is introduced to the notion of a business continuity plan and the importance of BCP for the organisation.

Once they are aware of the need for BCP, focus can be shifted towards the cyclic approach and the backup cycle in particular. The awareness exercise should also be focused more on general BCP education for the organisation and its employees.

Only those employees directly involved in plan creation need to be educated about the cyclic approach. Following the awareness exercise, it is necessary to appoint a BCP workgroup, or at least responsible individual to oversee the project. This is one of the steps that should obviously be completed only once seeing that the appointed individual will typically oversee all project cycles. To conclude the project planning for the backup cycle, project prospects, or cycle prospects in this case need to be identified. These include identifying all cycle objectives and cycle timeframes.

6.3.1.2 The Business Impact Analysis (BIA) phase

As this is the first cycle of the BIA for the continuity planning project, it is necessary to do a full analysis of all the business processes within the organisation. As the majority of organisational data is identified during the BIA phase, it is essential that the BIA is completed before the continuity strategies phase commences. This is because the gathered information is mostly used to identify the appropriate continuity strategies for the organisation. Therefore it is essential that all processes are identified, analyzed and prioritized. Disaster scenarios and supporting resources for each process need to be identified as well.

For this cycle, supporting resource identification is the most important step in the BIA pertaining to this cycle. The reason is that it directly influences the backup strategies determined in the following phase. It is, however, not possible to identify the most important resources without identifying business processes and their criticality and, therefore, all BIA steps are to be carried out during this cycle.

6.3.1.3 The Business Continuity Strategies phase

Having identified and listed the data considered critical, it should be ensured that this data is continually available or easily acquired, even in the event of a disaster. This is done during the continuity strategies phase by identifying the appropriate backup strategies. An organisation should, therefore, determine the appropriate backup method for its data and decide how the data will be transported offsite during this cycle.

Other steps belonging to the continuity strategies phase is not applicable to this cycle as they are related more to ensuring continuity of business processes and to the recovery of the IT department. They will consequently be addressed in subsequent cycles.

6.3.1.4 The Continuity Strategies Implementation phase

For this methodology, no physical procedures belonging to the continuity strategies implementation phase is applicable to the backup cycle. Therefore, the only step from this phase that can be incorporated into this cycle is the identification of a recovery team responsible for implementing the backup strategies. This team will generally be the technical recovery team as discussed in the previous chapter. It is possible that this step will not involve the identification of all team members.

This is because the technical recovery team will have many other responsibilities and these will most likely be addressed in the other cycles. Team identification will also depend on the number of teams an organisation decides to identify. It might be that an organisation decides to appoint a team solely for data backup and restoration.

6.3.1.5 The Continuity Training phase

Training during the backup cycle should include both introductory and detailed awareness training. The difference will come into play when the topic for training is chosen. The training should therefore cover only that which is applicable to the current cycle. For this methodology, that would include training covering the backup strategies only.

6.3.1.6 The Continuity Testing phase

The testing phase of this cycle will include only plans to test the backup strategies developed during this cycle. This phase will still involve the creation of test plans including issues such as test objectives, schedules, location etc. It will furthermore also be possible to conduct all specified types of tests. This is because the plan that exists now is a full business continuity plan, even though it is limited to a data backup and restoration plan.

Integrated testing would for example involve testing a combination of components that all involve backup and restore related activities, just as would have been done with a full and complete business continuity plan. A full test would function exactly the same, testing all the available components that exist at this stage.

6.3.1.7 The Continuity Plan Maintenance phase

The maintenance phase is the only phase that will have all its steps carried out during each cycle seeing that plan maintenance stays the same whether the plan is only a backup plan or a fully functional business continuity plan.

The maintenance framework for the example methodology includes steps to report identified changes, determining their impact, updating the plan if required and finally signing off on the changes by the appropriate individuals. Because all maintenance steps will be carried out independent of what cycle it is, the maintenance phase will not be discussed for succeeding cycles.

In the backup cycle and its various phases all steps that relate to organisational data backup should have been carried out. Therefore, once this cycle and all seven methodology phases have been completed, an organisation should have an effective data backup and restoration plan in place. This plan, if tested and maintained, should allow for the successful data backup and recovery. The following section will discuss the disaster recovery cycle and the methodology phases for this cycle. Many small organizations might decide that they only require a backup plan and need not continue with the methodology at that point in time.

6.3.2 The disaster recovery cycle

The main objective of this cycle is ensuring that IT can recover following a disaster. It is important to take into account that proper data backup and restoration procedures are in place already, as a result of the previous cycle. All seven methodology phases will be incorporated into this cycle, but the most important phases are the business

continuity strategies and strategies implementation phases. These phases, along with the others will be discussed in the following sub-sections.

6.3.2.1 The Project Planning phase

For the disaster recovery cycle, a reduced level of project planning is once again required. Management commitment must be obtained before the second cycle formally commences. Management should now be fully aware of the purpose of the BCP and will not need to be educated on the topic again. They will, however, need to be made aware of the project progress following the completion of the backup cycle. As mentioned in the previous chapter, if they are satisfied with the results, they will be more than willing to lend their support to this cycle and its activities.

Seeing that employees have already been educated about BCP in the previous cycle, no formal awareness-training step is needed. It is, however, not ideal to remove the awareness training completely from this cycle. It is always a possibility that employees, who have not yet been exposed to BCP, must be educated. To finalize planning, schedules and objectives, as done for the backup cycle, need to be set up. As mentioned in the planning section for the previous cycle, no workgroup or individual needs to be identified now.

6.3.2.2 The Business Impact Analysis (BIA) phase

Because a complete BIA has been performed during the backup cycle, all critical processes, resources and disaster scenarios have been identified. It is, however, not necessary to exclude the BIA phase from this cycle completely. There is always the possibility that new business processes might have been added or existing process information changed. Therefore, a BIA review should be sufficient to ensure that business process information is correct and up to date. This is, however, only a suggested step seeing that the maintenance phase should be sufficient to identify any important changes. The main information required from the impact analysis during this cycle would be Recovery Time Objective

(RTO) values for the business processes that will be used to identify the appropriate processing alternatives for the organisation.

6.3.2.3 The Business Continuity Strategies phase

As mentioned, the results from the BIA will once again be used as input for the continuity strategies phase. The identification of recovery alternatives for the various business processes will be determined by how quickly they need be up and running again. The RTO values for the various processes will, therefore, play an important role in this process.

6.3.2.4 The Continuity Strategies Implementation phase

To support the recovery goal for this cycle, continuity strategy implementation steps that should be incorporated are mainly the emergency response procedures and the recovery procedures. The emergency response procedures include notifying the appropriate plan participants and the plan activation conditions. Furthermore, to conclude the continuity strategy implementation activities for this cycle, an organisation has to identify teams responsible for all recovery related efforts. For the example methodology, this team would firstly include identifying those employees in the management recovery team who have the responsibility of receiving the initial disaster alert, determining when to activate the continuity plan etc.

Also, the user recovery team members required to perform tasks such as notifying the required vendors, verifying the status of employees after the disaster etc. should be identified. Finally, all those employees belonging to the technical recovery team and involved in typical recovery activities, should be identified.

6.3.2.5 The Continuity Training phase

As the case was with the previous cycle, training must once again be in detail for those directly involved in the recovery process as well as introductory training for the rest. The training should include all the IT recovery related topics. Employees

should be educated on alternate site procedures, emergency response procedures as well as IT recovery procedures.

6.3.2.6 The Continuity Testing phase

For the disaster recovery cycle, testing would involve verifying whether IT could be recovered in the desired amount of time. This of course depends on whether the organisation has chosen an offsite recovery solution or not. Also, along with recovery testing it would also be wise to test all aspects of the new plan, including the backup plans as well. This will test whether interrelated modules can be completed successfully, i.e. can procedures involving both recovery and data restoration be carried out successfully. Test plans must once again be created prior to testing. Organisations can once again carry out all the desired types of tests, producing a test report with test results afterwards.

Once the disaster recovery cycle is complete, an effective disaster recovery plan will be in place. Such a plan will include procedures that will ensure swift recovery of the IT infrastructure of an organisation.

Furthermore, seeing that a backup plan was created during the first cycle, the plan at this stage will include data backup and recovery procedures along with the IT recovery procedures that were identified during this cycle. Again, many smaller organisations might decide that a backup and recovery plan is adequate for their needs. The next cycle will concentrate on business process continuity.

6.3.3 The contingency planning cycle

The contingency planning cycle aims at ensuring the continuity of all critical business processes while IT is recovering. Once again the continuity strategies and strategy implementation phases provide the most important steps to accomplish this. The seven phases and how they differ for this cycle are discussed below.

6.3.3.1 The Project Planning phase

Just as for the previous cycle, project planning is necessary to ensure that the contingency planning cycle commences properly. Activities to be performed are virtually identical to the disaster recovery cycle. Management needs to be notified of project progress and if satisfied, they should commit to the contingency planning cycle and all associated activities. A formal high-level awareness exercise should be completed, as a number of employees, not being involved with BCP yet, need to be introduced to the subject. To finalize the planning for this cycle, cycle objectives need to be identified along with schedules for completing these objectives and thereby the cycle.

6.3.3.2 The Business Impact Analysis (BIA) phase

As the case was for the previous cycle, the completion of a full BIA is unnecessary and impractical. Performing a brief review of business processes and associated data should once again prove to be sufficient at this level of the BCP project.

6.3.3.3 The Business Continuity Strategies phase

For the contingency planning cycle, the factor that distinguishes it from other cycles once again comes into play during the continuity strategies phase. The goal of this cycle is ensuring continuity of business processes, and the continuity strategies step that supports this goal is mainly the user holding strategies step. These strategies specify employees' day-to-day responsibilities to ensure continuity later at a later stage.

6.3.3.4 The Continuity Strategies Implementation phase

For the contingency planning cycle, the main strategy implementation step involves the writing of process continuity procedures. These, as mentioned in the previous chapter, are the procedures that will help each process to continue (manually or otherwise) while IT is recovering. To conclude the strategies

implementation phase for this cycle, the necessary teams or team members have to be identified. In general this would include those individuals responsible for supervising the business process continuation process and recovery, as well as other related activities.

6.3.3.5 The Continuity Training phase

Training for the contingency planning cycle will involve introductory and detailed awareness training that will cover the basic user responsibilities (pre-disaster) as well as the business process continuation procedures that should be completed after disaster has struck.

6.3.3.6 The Continuity Testing phase

Contingency planning cycle testing should be no different than for the previous two cycles. Testing will only take longer as there is now a more complete continuity plan in terms of functionality than before. Again, all aspects should be tested to ensure that the plan is completely flawless. All available tests should be conducted to guarantee the above. If the plan is tested regularly it will ensure that all changes that might have affected the plan since the last set of tests are properly implemented. The same procedure must be followed as was done for the previous tests. This includes test plans, performing the tests and writing a report afterwards.

Once completed, the contingency planning cycle will have produced a set of procedures describing how business processes will be continued in the wake of disaster. Such a set of procedures, i.e. a contingency plan, will have been created for each process. This collection of contingency plans will complement the backup and recovery plans created in the preceding two cycles. The final cycle will be discussed next and will concentrate mainly on recovery and continuity supporting steps.

6.3.4 The continuity planning cycle

At this stage of the BCP project, the business continuity plan could be said to be nearing completion. This cycle will concentrate on the various steps that could not be directly attributed to one single goal such as continuity or recovery. Rather, they apply to all these previously established goals or related goals. These steps, along with their reasons for inclusion, will be discussed in the following sub-sections.

6.3.4.1 The Project Planning phase

To initiate the planning process for the final cycle, steps identical to those completed in the previous two cycles are required. Of these steps acquiring management commitment is, as for the previous cycles, the most important step. As for the previous two cycles, project progress needs to be relayed to management before they will commit to the final cycle activities. Once this is done, the cycle projects need to be determined as per usual.

6.3.4.2 The Business Impact Analysis (BIA) phase

A final review of the most important business process is suggested to end off the last BIA for the BCP project. This is once again to identify any new functions that should be added to the list of mission critical business processes.

6.3.4.3 The Business Continuity Strategies phase

Having progressed this far in the continuity planning process, all goals that directly address the continuity and recovery of the organisation have been covered. All that is left are those activities that support these goals.

These include insurance cover review, preparing for public relations and ensuring that emergency resources are available that could come in handy in a disaster situation. All these steps, therefore, need to be dealt with to finalize the continuity strategies for the BCP project.

6.3.4.4 The Continuity Strategies Implementation phase

To finalize the strategy implementation for the BCP project it requires only the necessary team and team members to implement the above-mentioned strategies. For this methodology, this would involve the identification of an administration recovery team and its members. The general responsibilities of this team would include insurance cover review, public relations, payroll activities etc. Once again, the required teams for this phase will depend on the teams an organisation have decided on to carry out recovery.

6.3.4.5 The Continuity Training phase

Finalization of the training process for the BCP project should include informing all participants on procedures relating to public relations, insurance coverage and policies for the organisations and the usage and location of identified emergency resources for disaster situations.

6.3.4.6 The Continuity Testing phase

At this stage in the BCP process the plan can be seen as being complete. This, however, only holds true until the next organisational change. This will fortunately be corrected by the maintenance phase. A set of tests ended by a full test can now be completed and when successful, an organisation can say with confidence that their plan can effectively recover the organisation to its original or close to original state.

Once the final cycle is complete, an organisation should be in possession of a full and complete business continuity plan. This plan will include procedures that describe how organisational data should be backed up and restored, how the IT infrastructure is to be recovered to an acceptable level, how business processes can continue operating and how the steps discussed in the above section can contribute to recovery and continuity. All that is required for the business continuity plan to stay effective is continued maintenance and testing.

6.4 Conclusion

This chapter discussed the cyclic approach for simplifying the implementation of BCP methodologies. This approach divides a methodology and its various phases into four separate cycles. These are, in order, the Backup, Disaster Recovery, Contingency Planning and Continuity Planning cycles. Each cycle had a different BCP related goal, and the seven phase methodology described in the preceding chapter was used to illustrate how a methodology can be implemented more easily. The motivation for these implementation cycles is that it will make it easier for small to medium sized organisations to introduce some aspects towards a complete BCP.

The first cycle, as the name states, concentrates on ensuring backups and information availability. All methodology tasks required to accomplish this are, therefore, reserved for the backup cycle. The Disaster Recovery cycle, as the name states, is set aside for those tasks that ensure IT recovery within the organisation. The Contingency Planning cycle aims to ensure that all business processes can continue as usual while IT is recovering and therefore all methodology steps aimed at business continuity will be completed during this cycle. Finally, the Continuity Planning cycle is reserved for accomplishing those tasks supporting BCP as a whole and not simply a goal as was the case with the other three cycles.

The following chapter will concentrate mainly on the maintenance of a business continuity plan. Continuity plans must preferably stay dynamic and continually up to date. Chapter 4 indicated that small to medium sized organisations in general are subjected to changes more often due to their dynamic environment and high rate of job creation. Therefore, a variety of possible organisational changes that could affect the business continuity plan will be discussed along with possible actions that could be taken by an organisation to ensure that these changes are reflected in the plan as soon as they occur.

Maintaining a Living and Dynamic Business Continuity Plan

7.1 Introduction

The cyclic approach to the implementation of Business Continuity Planning (BCP) was discussed in the previous chapter. It was described how the implementation of a BCP methodology could be divided into four separate sections or cycles to simplify the implementation process. Each cycle concentrated on a specific BCP related goal. These were, in order, the backing up of information, ensuring swift recovery of the IT department and continuing business process while the IT department was recovering. The final cycle aimed at accomplishing all methodology tasks not related to a specific cycle or goal such as recovery or continuity. These tasks usually supported BCP as a whole and included public relations planning, insurance cover reviews etc.

Once a methodology has been implemented the plan must be tested and regularly reviewed to reflect the ever-changing organisational environment. A complete continuity plan must, therefore, be dynamic in nature in order to give an accurate account of what the organisation looks like at a specific point in time (Wilson, 2000). If, however, it is decided that a plan will be reviewed every six months it could happen that in a worst-case scenario, the plan will be almost entirely outdated. (Johnson, 1998). The purpose of this chapter is to discuss how to ensure that the continuity plan becomes a living, dynamic document through employee involvement in maintenance activities. It will discuss what the possible changes are that could have an effect on the continuity plan and how to ensure dynamism regardless of these changes.

7.2 Organisational changes affecting BCP

Organisations operate in continually changing environments. New employees are constantly hired and current employees leave the company, are promoted or their details change. Organisations also tend to add business processes, or discard those that are outdated or perform a function that is no longer required. Changes such as these also affect other areas within the organisation such as work responsibilities and priorities for employees. A business continuity plan must reflect the current recovery and continuity capability status of the organisation. Therefore, both the organisation and continuity plan rely heavily on accurate and up to date information (Moore, 1995).

As a result of this an organisation must ensure that their continuity plans are regularly maintained to guarantee that they stay effective. Continuity plan maintenance procedures should also preferably be incorporated into the organisation's change management procedures (BS7799-1, 1999). This is to ensure that changes affecting BCP along with those affecting other areas within the organisation will be managed in a standard manner.

One method for identifying changes that affect BCP is the regularly scheduled review of the continuity plan to determine whether the plan still reflects the current organisational state. The frequency of these reviews differs from one organisation to the next and depends on how dynamic the organisation is. A second reason for making changes to the business continuity plan is due to organisational events that trigger the need for an immediate plan update (Glenn, 2002). The key to ensuring a continually updated continuity plan is communication. The entire organisation must realise the importance of keeping the plan updated and should cooperate in providing the relevant information to do so (Hagg, 2001).

These events that prompt the need for plan changes include, amongst other things, changes in personnel, equipment, procedures, vendors, software and organisational policies (Glenn, 2002). This section will discuss the possible organisational changes, the effect that they might have on the business continuity plan and suggested solutions to ensure that these changes are reflected in the continuity plan.

7.2.1 Changes in personnel

Personnel related changes could include growth or reduction in the workforce size of an organisation, the promotion of existing staff or simply changes made to employee details (Moore, 1995).

These employee-related changes could have an effect on a wide number of aspects related to the plan. The most obvious component that could be affected is the existing recovery team structure. This is not necessarily the case when employee details change, but when employees leave the organisation, or new ones are either hired or promoted it will require a definite change in recovery team details.

What the exact change would be will depend on the event that caused the need for this change. If, for example, an employee was promoted, one would have to ask oneself whether his or her current responsibilities will change completely, or whether new responsibilities are simply added. If, however, an employee left the organisation, the recovery team records would need to reflect this and a replacement would need to be sought as soon as possible. When a new employee is added to the payroll, he or she first of all needs to be given general BCP training. Then it should be determined what tasks and skills this employee possesses in order to figure out what role he or she will play in the BCP process. Once this is done, recovery team details and procedures need to be updated.

Having to update the recovery team details is probably the most obvious effect of changes in employees and their details, but further effects could also influence existing recovery or continuity responsibilities and emergency contact listings. As soon as any changes regarding personnel take place, an organisation needs to examine these areas of their continuity plan, more to determine the effect, if any, that these changes have to ensure the swift update of the continuity plan (BS7799-1, 1999). To ensure that personnel related changes are instantaneously reflected in the plan, various actions can be taken or controls can be implemented.

The first action is to build a measure into the system controlling all personnel changes for the organisation. Such a measure would alert and remind whoever is

responsible for updating personnel records, most likely the human resources department, to notify the responsible BCP coordinator of the change. It would then be up to the coordinator to determine what areas of the plan, if any, are affected by this personnel related change and then update the plan as required. As soon as the plan has been updated, the affected employees also have to be notified.

An alternative, or more automated approach to this solution is an automated message sent to the coordinator via e-mail containing some specifics about the change. Once again the responsibility would lay with the coordinator to affect the changes to the plan and letting the relevant parties know.

The second action involves either making use of the same database to store employee information and BCP information. This way, when employee details change it will automatically be reflected in the plan. Alternatively, if separate databases are used by the organisation to store employee and BCP information, a mechanism must be implemented to automatically update the BCP information when changes are made to the employee information database. In addition to this approach a message must still be sent to the BCP coordinator for notification purposes. The effect of these changes on the plan must after all still be determined manually.

7.2.2 Changes in hardware and software

Changes in hardware and software are also events that would most likely trigger changes in the business continuity plan (BS7799-1, 1999). It is common knowledge that both hardware and software become outdated and need to be upgraded or replaced. This unfortunately will most likely have an impact on the continuity plan and the information contained within. Organisational hardware and software are components that most business processes cannot do without (Guttman & Roback, 1995).

Should any hardware or software related changes take place the continuity plan must be updated as soon as possible. Areas that will be affected are amongst others hardware and software listing for each process as well as the hardware and software required for the alternate site solution(s) chosen by the organisation. Further

changes could involve continuity and recovery procedures as a result of activities performed by hardware that could, for example, have been done manually or by means of alternative equipment before. All the possible effects have to be considered and examined as soon as these changes take place.

One suggested solution for keeping software information up to date involves reminders that appear as soon as software is removed or added to the operating system registry on any standalone or networked computers. This will ensure that whoever installs or removes software will inform the BCP coordinator of these changes. Unfortunately the software details still need to be updated after installation or deletion. To ensure this, an organisation can allow these actions to trigger an obligatory message containing key software details to be sent to the coordinator.

An alternative to the above-mentioned would involve the required information to be entered by whoever installed or removed the software via an automatic popup information-gathering screen. This information could then be sent to the coordinator to determine the effect on the plan and the required updates should then be made to the plan as well as the BCP software information database. Wrobel (2000) suggests making use of a software inventory so that one can always know what software is used by the organisation and its critical equipment. Such an inventory could then be updated as soon as software details change in any way and the coordinator, once notified, could use it to update the plan appropriately. Once the plan has been changed all affected employees should be notified of these changes.

As the case was for the software, Wrobel (2000) mentions that a hardware inventory could prove useful to keep track of organisational hardware. An organisation could further also use such an inventory to keep track of hardware changes. The same principle could be applied to tracking hardware changes as have been suggested for software changes. Upon adding or removing a hardware device, or upon restarting the operating system, a popup alert could notify of the responsibility to inform the BCP coordinator. Alternatively, a message could be automatically sent to the coordinator containing key hardware information.

Installing additional hardware usually involves software installation and operating system restart as well and, therefore, a trigger mechanism should be simple to implement.

Removing hardware will not be that simple to detect. An organisation must, therefore, make sure that employees cooperate in keeping the coordinator up to date. It can even make employees responsible for any consequences resulting from failure to notify the coordinator of any changes, whether they affect the continuity plan or not. Furthermore, the hardware inventory must be updated as well when these hardware changes occur. Once again, this could be left to whoever is responsible for the changes in hardware to also update the inventory. This could in turn trigger a message to the BCP coordinator to update the BCP hardware inventory. If a common inventory is used for both hardware and BCP information, the coordinator must ensure that, if changes were made to the inventory, that they are correct before proceeding to update the continuity plan. Employees affected by these changes must then be notified about them and how they or their tasks are affected.

7.2.3 Changes in business processes

Organisations are constantly changing and growing environments. This usually means that new processes and operations begin while others are withdrawn (Moore, 1995). Both the addition and withdrawal of processes will require a thorough review of the continuity plan. As soon as any changes involving processes take place, the first obvious question would be how critical the process in question is to the organisation.

One would for example need to determine whether the new or withdrawn process affects the existing continuity and recovery strategies. If, for example, a newly added process has an extremely high impact for the organisation it might require a change in the current strategies to accommodate this process. In other words, a cold site strategy might no longer be adequate.

Not only will the continuity strategies be affected, but also the recovery teams and hardware and software listings. Employee details might also be affected if new employees are hired. If not, existing employees will most likely be given additional responsibilities, and this too will have to be reflected in the plan.

Senior management will most likely be aware of any new processes added and they should, therefore, be made responsible to make the relevant individuals aware of this new addition. The same could be said for the withdrawal of a certain process. The decision would rest with them, so they should start the updating process for such an event. Any changes to an existing process would require those involved in the process to react appropriately.

Adding a new business process would in most cases imply additional hardware, software and employees, just to mention a few. This could involve purchasing new hardware or software, or making use of existing hardware or software. Regardless, this would already trigger changes to the continuity plan. The coordinator must however be made aware of any new processes. The way an organisation can ensure this is to involve the coordinator in all or most business process discussions. This is however not to play an active or contributing role, but merely to stay aware of process changes. An organisation could even issue a policy statement indicating that the BCP coordinator must be present when final decisions concerning business processes are made. The business continuity plan can then be examined to determine the effect of changes, updates can be made and those employees involved in the changed portion must be notified.

7.2.4 Changes in vendors and suppliers

A change in vendors and suppliers is another event that could, or in most cases would trigger a change in the business continuity plan (BS7799-1, 1999). Various reasons could exist that would require an organisation to change vendors. They could, for example, no longer exist or an organisation may just no longer require services provided by a certain vendor. Areas that will be affected by such a change would most certainly be replacement lists for business process hardware and software, and general supplier listings for equipment and software. There is also a

possibility that business continuity strategies could be affected. This could be as a result of the recovery alternatives chosen being vendor maintenance agreement or quick shipping programs. As soon as such alternatives depend on services from a specific vendor, one has to review and alter the alternatives to reflect the changes in vendors.

As vendor related changes are not internal to the organisation, they will probably be more difficult to identify. An individual should possibly be made responsible to stay in contact or regularly monitor vendor availability. The responsible individual should create a dependable system of immediate awareness in the event that any vendor ceases operations, moves premises, amends contact details or merely discontinues some of its current services. An alternative is that an organisation could request to be notified by the vendors and suppliers themselves whenever changes occur, but certain vendors may not be that reliable. To prevent this, an organisation could possibly request a clause in the contract with a vendor forcing them to notify the organisation whenever changes take place, but that still means that the responsibility rests with someone not having a personal interest in the company, and the organisation has no control over their vendor information. Therefore, a better solution would be to make use of both methods, namely constantly monitoring vendors and also requesting that they report changes.

7.2.5 Changes in corporate policies and legislation

Any changes in the corporate policies also need to be evaluated to determine whether they affect the continuity plan (Glenn, 2002). Types of policies include the payment policies for staff during the disaster period, policies to assist employees and their families in disaster situations as well as all recovery and continuity related policies (Crimando & Steinberg, 1997). As there is such a large variety of different policies for organisations, changes in these policies in most cases are bound to affect the BCP within the organisation. For example, if management decides to create a new policy stating that any alternate recovery facilities need to be at least a certain distance from the main processing facility, the existing recovery strategies need to be reviewed and possibly changed to adhere to the newly created policy.

Usually when new policies are created or existing policies are altered, executive management is at the forefront of decisions concerning these changes. Therefore, management must be made responsible for notifying the relevant individuals of these changes. Also, besides corporate policies, legislation also changes from time to time. Any legislation that is applicable to the organisation must be identified beforehand and documented (BS7799-1, 1999). When any of these laws change, or new laws are created, they might affect the business continuity plan as well. Responsibility must, therefore, be assigned to keep track of new legislation or legislative changes, and how this affects the continuity plan.

As was the case with business process changes, management must be made responsible for informing the BCP coordinator of these changes. Once again it could even be included in the company policies that the coordinator needs to be notified of any policy related changes or even be involved in policy discussion meetings. Legislative changes however should be more difficult to monitor. Legal representation should most likely be used to ensure that the organisation stay on top of all new and changing legislation.

An appointed individual, or the BCP coordinator, should stay in contact with a legal advisor and an agreement could also be set up to ensure that the organisation is notified of any legislative changes by this advisor. The appointed individual or coordinator would most likely require a description of the new legislation or of the nature of the change to existing legislation. This would serve merely as background to determine whether it affects any of the continuity plan components.

7.2.6 Changes in the location of organisational facilities

Organisations tend to change the location of their facilities from time to time as well, whether these are offsite backup facilities, alternate processing locations or the main data processing facility (BS7799-1, 1999). Keeping track of such changes should not be such a complicated process. Upon first contemplating these changes they should be conveyed to the BCP coordinator and he/she should determine whether they affect any specific area of the BCP plan. A change of location of either the offsite backup storage location or alternate processing site will most

likely affect the plan and the strategies should therefore be examined if locations do change.

Once again, as the case was with some of the other changes, management would most likely be the first to know of such changes and they need to convey this to the BCP coordinator. As a move to another facility could easily disrupt operations, or at least those that are relocated, the continuity plan must be updated as soon as possible to include this change. Management must, therefore, be compelled to share this information with the coordinator, possibly through a policy statement as suggested in the previous sections.

The coordinator could now examine the existing plan to see how the change in location will affect the plan. This could include more than just moving existing equipment and installing software. If the acquisition of new equipment is necessary, the hardware inventory must also be updated, along with the software inventory, in case additional software is required. This all depends on the reason for the move to a new location. All this will need to be considered when the coordinator is notified of the possibility of the facility location change.

Various events could trigger changes in the business continuity plan. These were described in the sub-sections discussed. It was also suggested how an organisation could ensure that these changes are reflected in the continuity plan in a swift manner. Furthermore, some of these could have an effect on other areas of the plan. Therefore, it could be suggested that the entire plan is examined to determine whether one change could bring about other changes as well. Some changes might even require progressing through all seven methodology phases if it is certain that the change will affect a large portion of the business continuity plan. An event must, therefore, be evaluated to determine whether it is necessary to progress through the entire cycle again seeing that any size event could potentially alter other continuity plan areas.

7.3 Conclusion

Plan maintenance is an extremely important aspect of continuity planning. Organisations after all operate in dynamic environments and business continuity plans have to reflect this at all times to prove effective. Therefore, this chapter discussed, amongst other things, the various types of changes an organisation is subject to. These could include changes in employee data, suppliers and vendors, business processes, hardware and software, corporate policies and legislation, and the location of organisational facilities. It further discussed how these changes could have an effect on the business continuity plan and how an organisation can react to ensure plan dynamism.

The next chapter will address the critical role that employees play in the success of the recovery and continuity processes. Employee readiness will, therefore, be the main point of discussion and the chapter will examine how to go about ensuring continuous BCP readiness of employees.

Motivation and Continuous BCP Readiness of Employees

8.1 Introduction

The preceding chapter highlighted the importance of continually maintaining a business continuity plan. A continuity plan has to be as dynamic as the organisation it is written for. Organisations are constantly changing environments where employee, supplier, process, policy and a variety of other organisational aspects change on a regular basis. It was shown that the plan has to be reviewed both at recurring intervals as well as immediately following a significant change to ensure dynamism. Most employees have to be involved and various approaches were suggested to ensure this.

Ensuring that the business continuity plan is constantly up to date is unfortunately not the only post implementation issue that needs to be considered. This chapter will discuss the significance of continuous employee readiness in the continuity planning process.

Depending on the frequency of testing within the organisation, it is logical to assume that when BCP responsibilities are not exercised frequently, it could happen that employees become out of touch with their duties. The following sections will, therefore, discuss suggestions for ensuring that employees are continuously prepared.

8.2 Business Continuity Planning and employee readiness

Besides continuous maintenance, testing of the business continuity plan also figures into the equation. This is after all the only way to determine whether the plan will be sufficient to provide for business recovery and continuation. Testing is, however, an ongoing process. It is not a once off task and needs to be completed continually. This is not only to ensure that the plan will successfully recover and continue business, but also to ensure that

employees remain capable and ready to complete their designated BCP tasks (Johnson, 1998).

As discussed in the previous chapter, events that could trigger changes in the business continuity plan are not reserved for certain times of the year. Even though many sources specify that plan maintenance should be conducted once, twice or four times a year, events that require plan changes do not keep a fixed schedule. They could occur at any time and when they do, the plan will change. The problem with this is that although the plan is now up to date, it will have to be tested again to ensure that the plan is still effective after the changes were made.

It is for the above reason that some form of continuous BCP training and education is required to ensure that the entire organisation is kept up to date with the dynamic business continuity plan (Steinberg & Saracco, 1998). This section will, therefore, concentrate on methods and suggestions that will ensure that employees maintain their BCP readiness continually even if testing and training are not conducted often.

8.2.1 Involve employees in plan maintenance

One of the more obvious ways to ensure that employees stay ready is to make sure that they are always involved in updating the continuity plan. Not only does continuous employee involvement lower the cost of plan maintenance, but it also ensures that employees are up to date with their assigned responsibilities. This approach provides a variety of advantages. Firstly, as mentioned in the previous chapter, employees should be made responsible to notify the relevant individual(s) of any changes in their activities (Weems, 1999). This will not only ensure that each employee's section of the plan stays up to date, but that the entire plan stays dynamic in nature. By being made responsible to update the detail of the plan for which they are responsible, employees will have no choice but to stay continually ready.

Besides notifications of changes in operating procedures, employees will most likely update the existing procedures themselves. This will allow them to thoroughly familiarize themselves with their responsibilities.

Seeing that employees are responsible for writing their own continuity or recovery procedures, they should know and be able to recall their responsibilities easily in disaster situations. Adding new procedures unfortunately means that plans have changed and need to be tested. This, however, should not pose a problem seeing that employees do not need to familiarise themselves with these procedures, seeing that they wrote them. Therefore, being responsible for updating their section of the plan increases employees' BCP readiness.

8.2.2 Electronic Communication Systems and awareness

Electronic Communication Systems refer to technologies that aid information transmission and exchange such as e-mail, computer and video conferencing and the Internet in general. Many organisations are making use of it at present and this number is growing drastically with time. (Straus, Weisband & Wilson, 1998, p. 128-129). Organisations that need to keep employees up to date on BCP within the organisation could make use of the Internet, not just for general awareness, but also for more specific information (Crimando & Steinberg, 1997). Web sites, the organisation's intranet or even e-mail could be used to post the entire continuity plan or provide a means for employees to access or search for only the BCP information applicable to them.

If the most recent version of the continuity plan is continually available to all employees involved in the continuity planning process, they have no reason not to keep up to date with their responsibilities. However, only making the latest version of the plan available to employees through Electronic Communication Systems is not sufficient. An organisation must furthermore make certain that employees review BCP related information regularly. Employees must be made aware early in the BCP project of how important it is to perform their duties effectively when disaster has struck. They must be shown that poor awareness leads to poor performance. They must also furthermore be made aware of how a disaster could affect them and that they could be held accountable for their actions (Devargas, 1999, p. 44).

8.2.3 Using incentives to motivate employees

Even though up to date information is available to employees and they are aware of the importance of BCP both for them and the organisation, they may still need incentives to be totally committed to their BCP duties. Organisations often make use of an incentive or reward system to motivate employees. Reward systems or incentive schemes, in general terms, can be utilised by managers to compensate employees for work done. Rewards or incentive schemes can also be further categorized, with participation and performance being the two main categories (Steers & Porter, 1991, pp. 478-480).

Performance can be further subdivided into two more categories, namely the employees' expected role and also extra role behaviour. The expected role refers to the minimum expected performance as determined for employees, i.e. the normal daily responsibilities expected of them. The extra role behaviour refers to those activities performed by employees that are not expected of them by the organisation. This type of behaviour usually ensures that an organisation functions better than expected given that an adequate number of employees perform more than what is expected of them. It is, therefore, in an organisation's best interest to encourage extra role behaviour from employees (Steers & Porter, 1991, p. 481). Motivational methods in the form of rewards do not necessarily have to be in the form of cash or bonuses. The aim of the incentives scheme is to positively influence employees (Tyson & Jackson, 1992, p. 178).

Management can also consider these rewards or incentives to motivate employees to stay up to date with their BCP responsibilities. As mentioned, the continuity plan and each employee's responsibilities should be continually available and it is up to employees to maintain their readiness. Incentives to motivate employees could include bonuses when tests are conducted successfully, or when employee performance in tests exceeds expectations.

As mentioned, these incentives can also include non-monetary rewards such as additional leave for those employees who excel in their duties. Additionally,

organisations can decide to penalise those employees who are proven to fail in their duties as a result of neglecting to study their responsibilities effectively. Labour laws should most likely be studied carefully to ensure that these penalties do not infringe on an employee's rights.

8.2.4 Ensuring readiness through regular scenario training

Testing and exercising a business continuity plan is not only very costly to the organisation, but is in most cases disruptive to the day-to-day business. Careful planning is also necessary prior to each test (Maslen, 1996, p.28). For these reasons it is easy to see why the management of an organisation, especially smaller ones, could be reluctant to conduct tests often. Therefore, alternatives to testing have to be thought of to keep employees involved in the plan, on their toes.

Such alternatives could include weekly or fortnightly classroom type exercises that deal with hypothetical situations or small exercises that do not take long, such as disaster drills (Maslen, 1996, p.28). The organisation could decide to choose one or more processes to test every week. Departments could collaborate on this testing session. Such a session does not have to be long and will concentrate on the employee's reaction to a scenario that is thought up by the BCP coordinator and made public during the session. These sessions will also inspire creative thinking on the part of employees along with testing their BCP readiness, which will be useful in actual disaster situations. For smaller organisations, it might not be feasible to conduct weekly, or even fortnightly tests. These organisations must therefore determine a suitable timeframe.

8.2.5 Utilising job enrichment as motivational mechanism

Job enrichment is another available motivational mechanism that should keep employees on their toes and keep them committed. It involves giving an employee additional tasks making it clear that the emphasis is not on the increased workload.

Rather, the employees are made to feel more important and made aware of their accountability.

With job enrichment an employee becomes more actively involved in all the planning and appraisal activities related to their work. This mechanism also often involves the addition of more complex tasks and activities and these serve to increase the employees' expertise in their particular field or job. Studies have shown that this method was responsible for a noticeable increase in both employee morale and productivity. Absence of employees was also considerably lower (Tyson & Jackson, 1992).

It is felt that the above-mentioned motivational method can be just as well applied to motivate employees to stay up to date with their BCP responsibilities. This especially holds true because job enrichment has been proven to reduce employee absence (Tyson & Jackson, 1992). Absence of employees could after all seriously affect the BCP process. It has already been mentioned that job enrichment not only adds to the employee's importance in the workplace, but also makes them aware of their accountability. Even though their BCP responsibilities do not fall under their everyday work responsibilities, the organisation should still make it clear that neglecting their BCP related tasks could ultimately affect their and the organisation's future.

It must, therefore, be made clear to all employees that whatever restrictions exist in their everyday tasks, do not necessarily apply to their continuity or recovery tasks. They should be given latitude to an extent when it comes to their responsibilities. They could use their initiative, as long as their efforts contribute effectively and efficiently to the continuity and recovery of the organisation. Employees must feel that the responsibility of creating procedures for their continuity and recovery tasks is entirely up to them. They should, however, not be left completely up to their own device and their work should most likely be reviewed to see that it is in line with the rest of the plan and that the written procedures are indeed effective in ensuring continuity and recovery.

8.2.6 Utilising job redesign as motivational mechanism

Job redesign is another method designed to motivate employees in the workplace. Job redesign aims at utilizing an employee's individual skills with respect to judgement and decision-making. Those tasks that are repetitive in nature and more or less routine are completed by other means. Job redesign directly influences the career opportunities for the employee.

It increases the employee's productivity and labour quality, while reducing organisational costs and bottlenecks. Staff also seemed to become more flexible and was seen as a resource to the organisation. Short-term problems do include an escalation in training costs, but this changes, and cost decreases with time.

Personnel related advantages included improvement in recruitment and punctuality, as well as industrial relation and skills development (Tyson & Jackson, 1992).

Because of aspects such as an improvement in punctuality or reliability, and the fact that after job redesign an employee should be able to complete assigned responsibilities more efficiently, it should leave more time to concentrate on BCP responsibilities and review them more frequently. Further advantages, as have been mentioned, is increased productivity and skills development. Although these advantages are mentioned with respect to employees' daily responsibilities, they could most likely be applied to the employees' BCP responsibilities as well. The increased productivity issue would firstly allow more time for an employee to concentrate on the continuity planning responsibilities. Secondly, when an employee's level of productivity increases when performing his everyday tasks, it should be possible to apply this to his BCP tasks as well. Employees should, therefore, in theory, be able to perform their continuity or recovery tasks more efficiently after job redesign.

An improvement of skills development could also serve to increase employee readiness. The rapid improvement of employee skills would most likely mean that there would be a steady increase in employees' assigned daily tasks as their skill level grows.

Additional skills will most likely mean additional or new responsibilities, and consequently additional or new continuity planning responsibilities. Therefore, a high rate of increase in skill development will more than likely result in employees continually having to review additional or new BCP responsibilities.

8.2.7 Eliminate demotivator factors within the organisation

Besides implementing a variety of mechanisms to motivate employees to excel in their specific responsibilities within the organisation, the company must also consider eliminating most or the majority of demotivating factors. According to Tyson & Jackson (1992, p. 36) various factors that inhibit performance and innovation could exist within the organisation. Firstly, the environment in which the employee is expected to perform his or her tasks plays an important role. An organisation must, therefore, try to better the working conditions of employees seeing that satisfactory environments should lead to increased performance.

Other factors include inadequate training, conflicts between employees, leadership issues, insufficient staffing levels etc. Insufficient staffing levels are especially seen as a demotivator factor seeing that organisations often try to compensate for it by means of overtime. Even though employees might not have a problem with working overtime for a while, in the long run it might actually lead to a dramatic decrease in performance. Even the personal problems of employees could play a role and organisations have to take action to solve even these to ensure an increase in employee productivity (Tyson & Jackson, 1992, pp. 36-37).

Therefore, for the well being of the entire organisation and improving the BCP readiness of employees, organisations must take the above-mentioned factors into account. Staffing level must be reviewed to determine if they are currently adequate. Not enough staff could lead to each employee having too many BCP responsibilities, which could in turn lead to a decrease in BCP readiness and productivity.

The same could be said for the current working environment. If it is not satisfactory, it will not only lead to a decrease in productivity in the workplace. The results will most certainly be reflected in the performance of those employees' continuity and recovery responsibilities. Lastly, organisations will most certainly have to look after the emotional and physical well being of their employees, as this too will in the long run affect the state of BCP readiness within the organisation.

The above-discussed techniques were all aimed at ensuring that employees are motivated to keep up with changes to the business continuity plan, especially if these changes affected their role in the recovery and continuity process directly. Some of these techniques involved employee inclusion in plan development aspects, while others were purely motivational. Organisations utilising some or all of the above methods should succeed in keeping employees continually ready.

8.3 Conclusion

Ensuring that employees are constantly ready to perform their BCP duties could become a daunting task for organisations. It is an expensive exercise to conduct plan testing too often, even though it is the best way to keep employees ready for what is expected of them. Therefore, this chapter discussed various methods that could be utilised by organisations to keep employees prepared for what is expected of them in disaster situations.

The next chapter will be aimed at describing the development of a prototype demonstrating the workings of the cyclic approach as discussed in chapter 6. This prototype will illustrate how the seven phased methodology described in chapter 5 is implemented through four cycles. During each cycle, organisation information will be gathered and utilised by the prototype to make the necessary decisions and recommendations. Finally, it will be possible to produce a business continuity plan based on the gathered information.

BCP Cyclic: A Prototype Implementation of the Cyclic Approach

9.1 Introduction

Chapters 2 through 5 described the process followed in order to develop and describe an implementation approach for Business Continuity Planning (BCP) methodologies. This included an introduction to information security and BCP, a review of some current BCP methodologies, a discussion of Small to Medium Sized Enterprises (SME's), their characteristics that affect BCP and finally a discussion of a seven phased methodology based partly on the findings from the review and other relevant literature. The resultant methodology was then used to explain the cyclic approach in detail. This was done in chapter six. To further simplify the implementation of BCP methodologies, the proposed cyclic approach can be put into practice by means of a software tool. This, if proved to be successful, could serve as a valuable tool to small to medium sized organisations that normally do not have expertise in this regard available.

A tool of this nature will mainly illustrate how this implementation approach can be used to simplify the process of BCP in order to confirm its effectiveness in the working environment. This chapter will, therefore, discuss the development of a prototype, called BCP Cyclic, along with various development issues.

Sub-sections of this chapter will include a discussion on the specifications for such a tool, i.e. how it adheres to the requirements of the cyclic approach etc., what technical design decisions were made prior to the development of the package and what design decisions were required to ensure user friendliness. Finally, the chapter will conclude with a discussion of what improvements could still be made to make it an even better tool for building effective business continuity plans.

9.2 Adhering to the specifications of the cyclic approach

BCP Cyclic, once operational, aims to provide organisations, especially those that are smaller in stature, with a means to easily progress through a BCP related information gathering process. This process, however, would require information gathering to occur in several stages to accommodate those organisations not having the manpower and resources available to accomplish everything at once, as is done traditionally. This, as pointed out in chapter 6, is the objective of the cyclic approach. The cyclic approach is, however, just a concept specifying how an organisation could go about partitioning a BCP methodology. Implementing such an approach would, therefore, require the adoption of a suitable BCP methodology as well.

Therefore, one not only has to consider how such a software tool will subdivide a BCP methodology, but also how the selected methodology steps and phases will be completed. The tool will, therefore, need to contain some level of intelligent decision-making ability. This especially holds true for the Business Impact Analysis. Such a tool would, for example, need to find a means by which to prioritise organisational processes based on their identified criticality factors. Therefore, decisions often need to be made concerning how methodology phases and steps will be implemented via a software tool. As have been mentioned in some of the preceding chapters, methodologies do differ. Therefore the implementation of BCP Cyclic will make use of the methodology as discussed in chapter 5.

The BCP Cyclic prototype will, therefore, need to lead a user through all seven methodology phases in four distinct cycles. All this of course needs to occur in a user-friendly fashion. Therefore, a user must be able to understand at all time where they are in the entire process. Furthermore, the interface needs to be relatively intuitive so that even the inexperienced computer user will know how to go about progressing from one cycle to the next.

9.3 Technical decisions concerning the BCP Cyclic application

Having discussed the specifications for the BCP Cyclic application, a discussion of various technical decisions concerning its implementation will follow. These technical decisions were mainly influenced by factors such as development time, ease of interface

development and storage issues with respect to collected BCP information. Therefore, the main discussion issues for this section will include the motivation for the programming language used as well as the database chosen to store the BCP information.

9.3.1 Programming language motivation

For this specific project, the programming language found most appropriate was Microsoft Visual Basic. Firstly, it was found that interface development occurred much more rapidly and this is very important, specifically for the application in question. The BCP cyclic application, and especially the information-gathering wizard, consists of a relatively large number of screens each containing a variety of information inputs. The design of these screens, therefore, needed to be completed swiftly. Firstly, screen design forms a minor part of the entire application design. One would, therefore, rather spend more time on screen functionality than its design. Secondly, to ensure that application development is completed in the least amount of time, it is best to save time wherever possible. A good way to accomplish this is through rapid interface development, leaving more time for the functionality aspect of the application.

9.3.2 Information storage and the choice of a database

For information storage purposes, a relational database was chosen. This is because all of the gathered BCP information could be represented as tables. The relationship between these tables could also easily be represented using a database of this type. Seeing that the amount of information stored within each of the various tables and their fields within the database are not much, Microsoft Access was found to be more than adequate for database creation. The created database was also found to be easily accessible through Structured Query Language (SQL). The BCP Cyclic application depends a great deal on database access for frequent storage and retrieval of information. Furthermore, as BCP Cyclic is more suited for the single user environment. Therefore, databases such as Oracle that are suited for networking environments and large amount of data are not entirely necessary in this case.

The above sub-sections discussed motivations for some of the technical design choices of the BCP Cyclic prototype. These were the selection of a programming language and database to store the relevant BCP information. Ease and speed of development were seen as the main selection criteria. The next section will concentrate on certain design decisions that played an important role in the development process.

9.4 Design decisions for the BCP Cyclic application

The previous section discussed various specifications that need to be considered for an application of this nature. The next step is to discuss a variety of design issues that could ultimately affect the user friendliness and functionality of the application.

9.4.1 User interface design

When designing a user interface, especially in the case of the BCP Cyclic application, it is important to plan the screen layout carefully. This is so that the user will know what needs to be done at any particular moment and how they could proceed with operations having completed a specific task. The BCP Cyclic application, for example, makes use of a BCP information-gathering wizard that leads the user through the process of critical data collection. This immediately would indicate the necessity for a means to navigate back and forth through the collection of screens that represent each cycle. Furthermore, the methodology operations that need to be completed also differ from one cycle to the next. This means that not only should users be able to identify what cycle they are currently busy with but also the current position within the cycle at any specific moment.

The first method of cycle progress indication is through one of the main application workspace windows. These windows can be seen in figure 9.1. The BCP Cyclic application makes use of a Multiple Document Interface (MDI). This interface consists of three separate windows. The first of these two windows is utilised as a business continuity plan index that simplifies plan component accessibility. The second window is used as a means of displaying a plan once information gathering is completed.

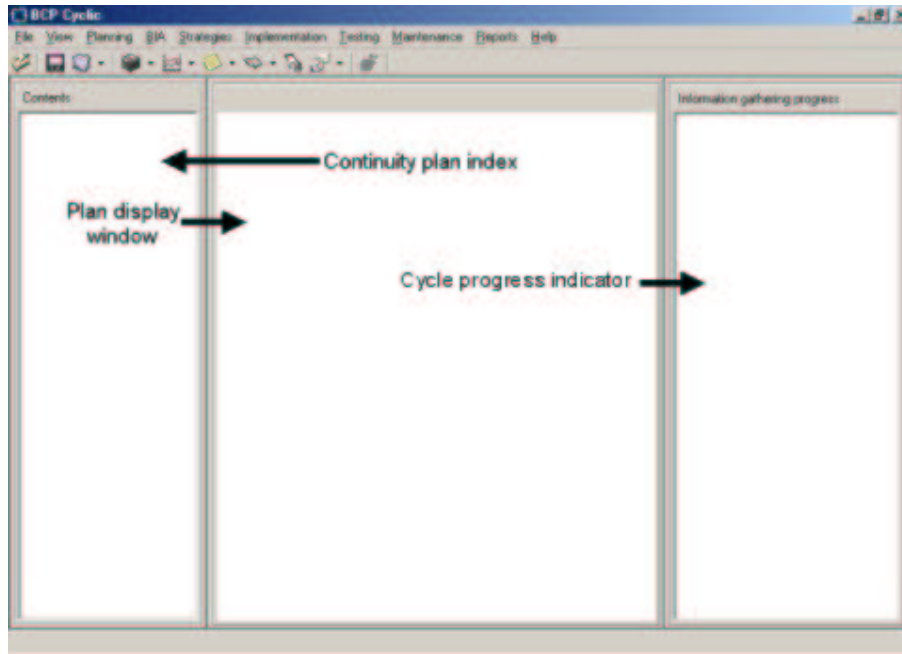


Figure 9.1: An example of the BCP Cyclic MDI

Depending on the current cycle, this built plan could range from simply being an organisational backup plan to a complete business continuity plan. The third window, which serves as a cycle progress indicator, as the name states, indicates for each cycle what methodology steps have been completed. However, a user could not determine what methodology steps are to follow by means of the cyclic progress indicator alone. Therefore a user cannot get a complete indication of methodology progress. For this reason a methodology progress indicator has been incorporated into the information-gathering wizard. This progress indicator gives a complete view of each methodology phase while a user traverses it. Even methodology steps not applicable to a specific cycle are shown, but greyed out. This is done to reveal to the user which methodology steps are still to follow in subsequent cycles or have already been completed in the preceding cycles. This approach gives a better understanding of the overall information gathering progress. The BCP Cyclic progress indicator can be seen in figure 9.2.

Together, the information gathering wizard progress indicator, along with the cyclic progress indicator, gives the user an exact indication of their BCP information gathering progress. Besides maintaining a visual log of the information gathering progress, user friendliness issues include providing the ability to constantly alter and maintain existing BCP related information. This could be done through the main menu and its submenus as well as various toolbar buttons, all located on the BCP Cyclic MDI. These menu options and toolbar allow the user to alter stored information without needing to invoke the

information-gathering wizard. This is especially useful in situations where minor changes need to be made to specific sections of the business continuity plan.

9.4.2 Keeping track of the information gathering progress

The previous section discussed various design issues with respect to maintaining a certain level of usability of the BCP Cyclic application. Two of these were the provision of a cyclic progress indicator and an information gathering wizard progress indicator. Seeing that for each of the four available BCP cycles a user could be involved in one of seven methodology phases, serious thought had to be given to the implementation of this concept. This sub-section will, therefore, discuss the techniques utilised to ensure effortless methodology traversal.

Implementing the cyclic progress indicator required a means to uniquely identify each of the list elements. The reason why each element had to be unique is because some list elements are present in all four cycles. For example, a user has the ability to perform a Business Impact Analysis or update business process details in every cycle. This means that for each cycle, the list identifier had to be unique in order to distinguish it from previous cycles.

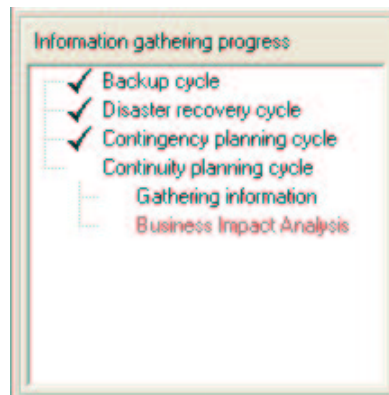


Figure 9.2: A cycle progress window

For the information gathering wizard progress indicator, keeping track of progress is slightly simpler. The wizard mainly makes use of the boldface property of text to indicate the progress within each methodology phase. Therefore the decision of what information to display once a user decides to proceed with a certain methodology phase is based on the state of the text listing the methodology steps for each phase. Such a steps listing can be seen in Figure 9.3.

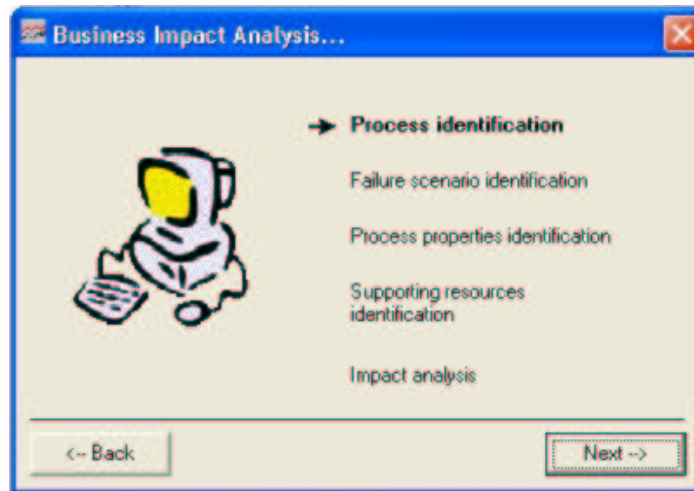


Figure 9.3: An information gathering wizard progress indicator

Consequently, to determine the BCP Cyclic application's behaviour when the user clicks the next button, the listing of methodology tasks are firstly examined. Once it is evident which task is to follow, the boldfacing is removed from the currently selected item and the next list item is bolded. Careful planning is however needed to ensure that once a specific operation is completed, the correct items' text properties are altered to reflect the progress.

A further section where current progress plays a very important role is the plan building process. A plan can be built as soon as a cycle has been completed, whether this is the Backup, Disaster Recovery, Contingency Planning or Continuity Planning cycles. This process involves constructing a plan by using the information currently in the BCP Cyclic database. The contents of this plan depend on the current cycle. This means that a plan built once cycle 2 is completed would contain information gathered during the previous cycle, as well as cycle 2 information. The plan will, therefore, grow as the information gathering process progresses from one cycle to the next. Therefore, BCP Cyclic required a method with which to ensure that for a certain cycle only the information pertaining to that and previous cycles will be included in the plan produced. When a user starts a new cycle, the current cycle number, i.e. 1 if it is the Backup Cycle, is automatically stored, and this stored value is then used to decide which plan building procedures are executed.

Various plan build procedures are grouped according to the cycle they belong to. As the cycle number grows, the plan building procedures will include those from the previous cycles as well as those belonging to the current cycle. The next subsection will discuss other design issues that affect and improve the user friendliness of specifically the BCP Cyclic application.

9.4.3 Assisting the user in information gathering activities

In a specialized application, such as the BCP Cyclic prototype, it could happen that application users do not have the necessary BCP experience to know exactly what is required from them. This especially holds true for the information gathering session. Even though the application has been designed to be user friendly, some BCP related terms that are, and have to be, used could make questions and tasks difficult to understand. It is also not ideal to force users to invoke the online application help each time a task is unclear.

Therefore, in those screens where tasks could appear unclear or ambiguous to some users, on screen text guidance has been included. This will guide the user, telling them what needs to be done and in most cases how to accomplish this. An example of this can be seen in figure 9.4.

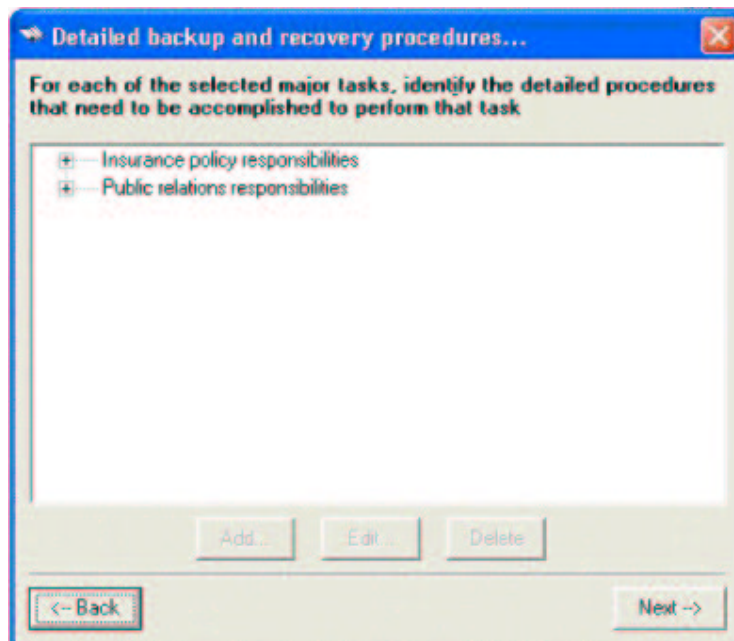


Figure 9.4: An example of on-screen text guidance

9.4.4 Guiding the user towards the right choices

In most software applications there are always actions that users are prohibited from performing prior to other actions that need to be completed before them. It is, however, not ideal to limit users' choices in such a way that it forces them to perform operations they are either not meant to, or willing to, perform. The BCP Cyclic application therefore, as far as possible, allows users to make the decision what actions to perform. This is not always possible seeing as in extreme cases a user must be forced to perform certain actions before they can continue.

An example of this would be using pop-up messages simply to alert users of the effect of their actions while still leaving it up to them to make the decision. In the maintenance phase of each cycle of the BCP Cyclic application users are allowed to review all gathered information and alter it where necessary. This involves a review of all gathered information. If a user chooses to proceed with operation even though maintenance is not completed, they will be made aware of this and asked whether or not they would like to continue. An example of a warning can be seen in figure 9.5.

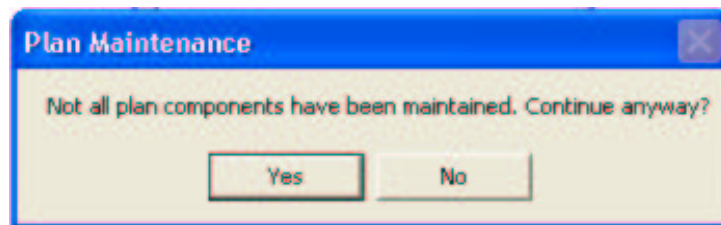


Figure 9.5: A warning message

This section concentrated on various design issues aimed at ensuring that the BCP Cyclic prototype is user friendly and functionally correct. These design issues included keeping the user continually updated on cyclic and methodology progress, along with assistance for more complex information gathering activities. The next section will discuss some of the shortcomings of BCP Cyclic along with the required improvements.

9.5 Possible improvements for the BCP Cyclic prototype

The main purpose of the BCP Cyclic application was the implementation and testing of the cyclic approach. Therefore, the application's functionality was not as important as achieving success and proving that such an approach could ultimately simplify methodology implementation and business continuity plan creation. Furthermore, as the BCP Cyclic application is merely a prototype at present, it is logical to assume that certain functionalities will be lacking and others that are present can be improved somehow.

9.5.1 Lack of printing capability

The first functionality lacking is that of a printing facility. The reason for this is because of the choice of programming language. Experience has shown that Microsoft Visual Basic does not provide the programmer with a lot of control over the coding of printing functionalities. Built-in printing functions do not provide adequate functionality for printing operations, especially for an application of BCP Cyclic's nature. Another factor directly affecting the printing capability is the lack of word processor-like facility for the application in question. Seeing that one of the objectives of this prototype is to produce a plan based on gathered BCP information, a user would expect formatted output and also expect this output to be printable. Unfortunately, the addition of such qualities to the prototype is a timely and complex process and also beyond the scope of this project. Therefore, once the plan is produced the BCP Cyclic prototype provides the user with the ability to save any generated documents in Rich Text Format (RTF). Such a saved document could then be edited appropriately and printed by means of any word processing application.

9.5.2 Representation and gathering of non-standard information

Further improvements are more applicable to the BCP information gathering exercise and in how much detail it is carried out. An example is the gathering of user holding strategy information. The BCP Cyclic prototype firstly requires the selection of a specific business process. Once this has been done, the various strategies for that process must be identified. Implementing this functionality is,

however, not easy. Organisations and their business processes often differ dramatically and this means that the nature and type of holding strategies will also differ. For any one process, the holding strategies could, for example, include the printing of various reports to be used in a disaster situation. Taking this into account, one would ideally, along with each strategy, like to store information about that strategy, such as the amount of reports printed along with where they are stored.

Implementing this specific example would be simple enough, but given the sheer amount of different strategies that could possibly exist and the information that needs to be stored about each option makes it complicated to design a standard screen where information of this nature can be entered. This problem can also be applied to various other sections such as continuity procedures, recovery procedures etc., where what can be done differs from one process or employee to the next.

The above sub-sections discussed various improvements to address some of the limitations of the BCP Cyclic prototype. It was mainly found that the prototype lacked functionality with reference to BCP information output. Furthermore, some the information gathering methods utilised proved not to be as effective as required.

9.6 Conclusion

This chapter discussed the development of a software prototype based on the specifications for the cyclic approach to BCP. This application was aimed at producing a business continuity plan by gathering information through four separate cycles. It was also mentioned that once each cycle was completed the prototype could build a plan based on the information gathered by that specific cycle. The chapter furthermore discussed various technical decisions such as the choice of programming language and the database chosen to store the BCP information. Design decisions were also discussed and included, mainly decisions to make the application more user-friendly. Finally, the chapter concluded by pointing out some future improvements for the BCP cyclic prototype.

Even though a prototype has been created to emulate the workings of the cyclic approach, it has not undergone any form of testing whatsoever. Therefore, it would be ideal to expose the BCP Cyclic application to a real case study in order to point out where exactly improvements can be made and how effective it is to accomplish the task it is intended for. The next chapter will discuss such a case study along with the various resulting findings and suggested improvements to the prototype and methodology.

Case Study

10.1 Introduction

Chapter 2 through 6 discussed the process of simplifying the Business Continuity Planning (BCP) process for small to medium sized organisations. This included the identification of characteristics that BCP methodologies should adhere to, to prove effective. Smaller organisations were also examined to determine the effect that their unique characteristics would have on BCP. In light of this, a detailed, scalable BCP methodology, that is suited to both small and large organisations, was developed along with a cyclic implementation approach to simplify methodology implementation. Finally, the methodology and implementation approach was implemented by means of a software prototype, which was discussed in the preceding chapter.

To determine the effectiveness of the prototype, along with the developed methodology and implementation approach, it was tested in a live, small business environment. This was done to identify the successes and shortcomings of the methodology and the prototype. It was further attempted to determine whether the cyclic approach is effective in simplifying methodology implementation. This chapter will discuss the nature of this exercise and the findings resulting from the case study.

10.2 Case Study objectives

The BCP Cyclic prototype, based on the seven phased BCP methodology and cyclic implementation approach, has up to this point not been formally tested and is strongly founded on theory. The developed BCP methodology has been based on existing BCP methodologies and their strong and weak points, thereby only in theory having the traits of an effective BCP methodology. An identical statement could be made about the cyclic implementation approach. It is, therefore, imperative to determine whether such a methodology and implementation approach will indeed prove effective in practice.

The objectives of this case study are, therefore, firstly be to determine how effective the BCP Cyclic prototype is in the environment it is mainly intended for, namely a small business environment. Secondly, the BCP methodology and implementation approach will be evaluated separately from the prototype to ascertain whether they are effective or not. The BCP Cyclic prototype will also benefit from any suggested improvements from the outcome of this case study.

10.3 The nature of the Case Study

The BCP Cyclic prototype has been tested in a relatively small organisation that suits the criteria of a Small to Medium Sized Enterprise (SME). The organisation has, however, requested that its name and other organisational information be kept confidential. For this reason the organisation in question will be referred to as Organisation A in this research dissertation. Organisation A has a small employee base and an IT infrastructure consisting of a file server, a small collection of pc's and some peripheral devices. Communication with customers and company franchisees plays a very important role in the day to day functioning of Organisation A.

The BCP Cyclic prototype was not operated by Organisation A employees due to the fact that it was still in development stages and would furthermore require users to be trained on its usage. There was unfortunately not ample time to do so. Instead, an information gathering exercise, based on the logical order as followed by the prototype, was utilised. This exercise gathered information pertaining to information backup and restoration, disaster recovery activities, contingency planning and finally BCP, separately. Results from the information gathering exercise were then entered into the prototype database at a later stage via the BCP cyclic interface. The next section will discuss the case study process in more detail.

10.4 The Case Study process

Seeing that Organisation A is relatively small, one person was appointed business continuity coordinator, as advised in the BCP methodology. All communication took place via this coordinator. Once the preceding step was completed, the BCP Case Study was initiated with an information gathering exercise. Employee, equipment, software and

vendor information was requested from the coordinator. Business processes were then identified and the information from the previous exercise applicable to each business process was identified. These processes were prioritised based on their criticality, and once completed, Organisation A's backup strategies were reviewed, and detailed backup procedures were established. Identifying an individual responsible for backup and recovery seemed sufficient due to a simple IT infrastructure, supported by the scalable methodology stating that smaller organisations can make use of one to two member teams. This concluded the backup cycle and a simple backup plan was produced.

The disaster recovery cycle commenced with a discussion of applicable recovery alternatives and the selection of an effective solution based on the business impact analysis. No further information gathering or business process reviews were necessary. The solution chosen was a mirrored site seeing that the existing infrastructure is not that complex or expensive to implement. This eliminated the need for further recovery procedures relating to equipment replacement. A disaster recovery plan was created once the cycle information gathering and activities were completed.

The contingency planning cycle largely involved identifying the process continuity tasks for each process. Employees assisted in providing the necessary information about their tasks for each process. Further activities included identifying documents that needed to be created on a regular basis and stored at the alternate processing location. Once again there was no need to establish further recovery procedures seeing that the operation was small enough to simply relocate to the alternate site if required. A contingency planning cycle plan was produced following cycle activities.

Finally, continuity planning cycle activities were commenced. These mainly involved identifying an individual responsible for public relations and a review of insurance policies and their coverage. No emergency resources were required for continuing operations. A business continuity plan was produced following the continuity planning cycle.

10.5 Findings and suggestions

The aim of the case study performed at Organisation A was to firstly determine whether the cyclic approach could effectively be used to implement a BCP methodology within

smaller organisations. In doing so, the BCP Cyclic prototype would also be tested to ensure usability, along with the chosen seven phase methodology to ensure both scalability and effectiveness. The cyclic approach proved very useful in the sense that it focussed on specific BCP aspects such as backups, disaster recovery etc., allowing one to concentrate more on these specific aspects. Below is a listing of further findings and suggestions brought about by the case study:

- The seven phase BCP methodology, to promote scalability, suggests that for smaller organisations less costly alternate processing options should be considered. It was, therefore, stated that expensive solutions such as mirrored and hot sites should be ignored completely by small companies. This was, however, found to be a more complicated choice than suggested by the methodology. It was found that small organisations needed to examine their IT infrastructure needs to identify a suitable solution, and in some cases a mirrored site might even be cost effective enough to implement. The BCP methodology, therefore, needs to be updated to reflect this, as well as the BCP Cyclic package.
- It was found that BCP Cyclic's approach to setting up backup schedules for organisational files was not effective. It involves the identification of critical files that needs to be backed up for each business process. Organisation A, however, archives only those files that have changed and, therefore, does not identify specific files, as done by the BCP Cyclic package. The software package consequently needs to be updated to ensure that image backups, i.e. selecting entire disks or file collections for backup, are catered for as well.
- The backup and recovery tasks at present do not consider the recovery alternatives. This means that when the detailed procedures are written to restore organisational data to its original state, one must consider whether it would be necessary to reinstall systems software, application software and the backed up data, or just the backed up organisational data. A mirrored or hot site solution would, for example, require no data restoration (if data is completely mirrored) or, worst case, only require the restoration of backed up data. The cyclic approach, therefore, may need to be reviewed to ensure that during the backup cycle consideration is given to the type of alternate processing solution that the organisation might choose.

- The BCP Cyclic package focuses largely on business processes and their properties, i.e. on the effect of their unavailability, important process resources, etc. The problem is that a variety of organisational resources (documents, files etc.) cannot be attributed to a single process, but rather to the entire organisation. The package must, therefore, be updated to accommodate these resources.
- The output produced by the BCP Cyclic package at present follows the structure of a combination of various existing business continuity plans or their contents listings. There is, however, a question as to whether a standard format exists for these plans. When queried about this, Organisation A was also not sure of how such a plan should look, or of the plan format they required. Further research, therefore, needs to include a study of how to partition a business continuity plan in such a manner that it would be of great use to an organisation, in both pre- and post-disaster situations. The BCP Cyclic package would then need to be updated to produce the desired output.

While conducting the case study, a number of findings regarding the cyclic approach and the BCP Cyclic prototype came to light. These issues, as discussed in this section, can contribute to a more effective methodology and software solution once implemented.

10.6 Conclusion

This chapter described the process of conducting a case study in a relatively small organisation with the main purpose of evaluating the cyclic approach along with the BCP Cyclic prototype. The results were mainly positive, proving that the cyclic approach is, though having been shown not to be perfect, effective in implementing a BCP methodology in smaller organisations. It can, therefore, be claimed that the scalable BCP methodology, as discussed in chapter 5, along with the cyclic implementation approach, can assist a small to medium sized organisation in creating a solution that will effectively address their disaster recovery and business continuity needs.

Improvements for both the cyclic approach and software package have been suggested. Once these changes have been implemented, the BCP Cyclic package should sufficiently enable a small to medium sized organisation to produce a plan ranging from a simple backup plan to a full business continuity plan.

Conclusion

11.1 Introduction

The development of the IT industry, including network environments and computers, is rapidly evolving, along with information security and technology. Information security plays an important role in protecting an organisation and its critical business processes. Advances in distributed systems, especially the Internet, have caused management to focus their attention predominantly on organisational threats and the possible effects they might have (Yngström & Carlsen, 1997, pp.3-8). Nowadays business functions must be continually available and organisations are increasingly becoming aware of this (Douglas, 1998).

Organisations are competing globally these days and their information technology resources and services need to be continually available (Glorioso & Desautels, 1999). Unfortunately organisations are all susceptible to disasters and unforeseen events and, therefore, typically need well-designed and properly tested business continuity plans. These plans ensure that an organisation's assets, operations, commitments and relationships throughout the organisation are kept in tact. This is important for ensuring business continuity (Moore, 1995).

To produce consistent and comprehensive business continuity plans, organisations must preferably adopt a suitable Business Continuity Planning (BCP) methodology. BCP methodologies generally guarantee that the creation of plans for the various business processes is coordinated properly. A variety of continuity planning methodologies are available, but unfortunately they differ quite extensively in application. The selection of a suitable methodology could, therefore, be a difficult process.

A further possible consideration is the size of the organisation when choosing a methodology. Chances are that smaller organisations with their limited resources and distinguishing characteristics might need a different methodology or at least need a

different implementation approach. Therefore, a methodology that is both detailed and scalable would prove invaluable to these smaller organisations along with an implementation method to further simplify methodology implementation.

11.2 Summary

The process of identifying a detailed but scalable BCP methodology commenced through the study of four known BCP methodologies. These were discussed in detail and analysed in terms of their advantages and drawbacks. This analysis, as discussed in chapter 3, assisted in the identification of criteria for an effective, ‘improved’ methodology.

Having identified the general requirements of a BCP methodology, the specific needs of smaller organisations with respect to BCP were examined. For this reason, chapter 4 discussed the characteristics of and classification methods for small to medium sized organisations. These characteristics were then studied in line with BCP requirements to determine how BCP would differ for smaller organisations. It was seen that existing, detailed BCP methodologies had to be altered in some cases to cater for the specific needs of smaller organisations. Based on the findings from these two chapters, a detailed BCP methodology, suited specifically to small to medium sized organisations, was identified.

This methodology, as described in chapter 5, was made scalable so that both large and smaller organisations would be able to implement it. This was done seeing that both small and large organisations typically have to address the same major issues. Some of the methodology steps, as discussed in chapter 4, were found to be more suited to large organisations. This typically meant that the same detailed methodology could be implemented by both large and small organisations. Those steps that do not apply to an organisation could simply be omitted.

Besides the need for a scalable methodology, chapter 4 also indicated that, based on the fact that organisations in general differ quite extensively, an implementation method would prove useful as well. Firstly, such a method would allow smaller organisations to implement a methodology with limited resources. Secondly, it would allow for partial implementation in cases where organisations need only certain BCP aspects to be in place. This implementation approach, entitled the cyclic approach, was discussed in chapter 6 and

involved partitioning a detailed BCP methodology into four separate cycles for simpler implementation. Figure 11.1 illustrates how the methodology is partitioned.

Both the cyclic implementation approach and the BCP methodology from chapter 5 were then implemented by means of a software prototype. The mechanics of this prototype was discussed in chapter 9. By means of a case study the prototype was then tested, mainly to determine whether both the methodology and implementation approach was effective. The results achieved were mainly of a positive nature, even though some possible improvements to the methodology, cyclic approach and prototype have been identified.

Further discussions in this study, though not incorporated into the prototype, shifted focus to the involvement of employees in the BCP process, especially with respect to maintenance and employee preparedness. These two aspects were examined in chapter 7 and 8.

		Backup Cycle	Disaster Recovery Cycle	Contingency Planning Cycle	Business Continuity Planning Cycle
Project Planning	1. Ensure top management commitment	✓	✓	✓	✓
	2. Conduct a high level awareness exercise	✓	✓	✓	✓
	3. Establish a BCP committee	✓	✓	✓	✓
	4. Determine project prospects	✓	✓	✓	✓

Business Impact Analysis	1. Identify critical business processes	✓	✓	✓	✓
	2. Identify failure scenarios	✓	✓	✓	✓
	3. Determine recovery time and point objectives	✓	✓	✓	✓
	4. Prioritising business processes	✓	✓	✓	✓
	5. Identify supporting resources	✓	✓	✓	✓
Business Continuity Strategies	1. Identify backup strategies	✓			
	2. Identify processing alternatives		✓		
	3. Identify user holding strategies			✓	
	4. Insurance cover review				✓
	5. Public relations				✓
Continuity Strategy Implementation	1. Identify emergency response procedures		✓		
	2. Write process continuity procedures			✓	
	3. Write recovery procedures	✓	✓	✓	✓
	4. Establish continuity planning team structure	✓	✓	✓	✓

Training	1. Introductory awareness training	✓	✓	✓	✓
	2. Detailed awareness training	✓	✓	✓	✓
Testing	1. Develop test plans	✓	✓	✓	✓
	2. Conducting tests	✓	✓	✓	✓
	3. Analyse results	✓	✓	✓	✓
	4. Write test report	✓	✓	✓	✓
Maintenance		✓	✓	✓	✓

- ✓ Indicates steps that must be completed
- ✓ Indicates optional steps or reviews

Table 11.1: Methodology subdivision by means of the Cyclic Approach

11.3 Limitations of dissertation

One of the biggest limitations of this study, and more than likely all studies of this nature, is the difficulty in gathering information. Firstly, although BCP information is in abundance, information that specifically relates to small and medium sized organisations is mostly not readily available. Secondly, conducting a case study could prove challenging, also due to information gathering difficulties relating to inability of employees to always provide the required information. This could be as result of various reasons of which company policy and an extensive employee workload are the two most common.

Limitations such as these need to be addressed or considered in future research, along with issues that will be discussed in the following section.

11.4 Future research directions

Chapter 3 included a review of various existing BCP methodologies, along with their strong and weak points. To ensure that these methodologies are correctly critiqued, it would have been advantageous to evaluate them from both an ontological and epistemological perspective as well. Furthermore, although the BCP methodology suggested in chapter 5 proved to be reasonably effective, some suggestions for improvement have surfaced during the case study exercise. The same holds true for the created prototype. Therefore, the above-mentioned improvements could provide for a more effective solution and should therefore be addressed at a later stage.

11.5 Conclusion

The aim of this study was mainly to determine how the BCP process could be simplified for smaller organisations with limited resources. To do so, the characteristics of small to medium sized organisations were studied to establish what sets them apart from large organisations. These characteristics were then incorporated into a BCP methodology, based on various existing BCP methodologies, to make it scalable. In addition, the methodology was supported by a cyclic implementation approach that further simplified the implementation process for smaller organisations. Both the methodology and cyclic approach were tested, by means of a developed software prototype, in a live business environment. Through this case study it was proven that the methodology and implementation approach are effective and can be used with great effect in the BCP process for smaller organisations.

By means of the above-mentioned case study, a few possible improvements to both the methodology and prototype have surfaced. Therefore, the methodology should firstly be reviewed and updated. Seeing that the prototype is closely based on the methodology, methodology related changes must further be reflected in the prototype as well. Furthermore, the non-methodology related changes must be made to the prototype. These

include updates to the information gathering and other procedures shown by the case study to have room for improvement.

In addition, the BCP Cyclic prototype needs to be further developed seeing that it is only in its prototype stage. This will include making the various updates that still lack, as described in chapter 9. Once completed, these changes will ensure that the prototype is user friendly and can be distributed and used by organisations to create detailed business continuity plans. Further considerations will include incorporating what was discussed in chapter 7 and 8 into the BCP Cyclic software package.

List of References

- Barclay, R. S. (2002). Do Small, Medium Companies Implement Disaster Recovery Plans? Disaster Recovery Journal [online]. [Cited October 18, 2002] Available from Internet URL <http://www.drj.com/articles/sum02/1503-11.html>
- Barrow, C. (1993). The Essence of Small Business. Great Britain: Prentice Hall Inc.
- Baruch, S. B. & Baruch, M. E. (2000). The Value Triad: Integrating BCP with Quality and Performance. Contingency Planning & Management. [Online]. [Cited October 19, 2002] Available from Internet URL http://www.contingencyplanning.com/article_index.cfm?article=319
- Beckmeyer, M. (2001). BCP at Small and Large Companies. Contingency Planning & Management. [Online]. [Cited October 19, 2002] Available from Internet URL http://www.contingencyplanning.com/article_index.cfm?article=379
- Besoft (2003). Company-Statement. [Online]. [Cited February 20, 2003] Available from Internet URL <http://besoft.be/index.php4?cat=company&cat2=statement>
- Boddington, T. (1998). Preparing for BS 7799 certification: Guidance on implementation requirements to organisations preparing for certification. London: British Standards Institution
- Bowler, A. & Dawood, M. S. (1995). Entrepreneurship and Small Business Management. Cape Town: Nasou
- BS7799-1. (1999). Information security management – Part 1: Code of practice for information security management. London: British Standards Institution
- Business Blue-Book of South Africa. (2001). Cape Town: National Publishing Pty Ltd.

- Business Contingency Preparedness (2002). Glossary of Contingency Terms.
[Online]. [Cited May 11, 2002] Available from Internet URL
<http://www.businesscontingency.com/glossary/html/glossary.htm>
- Button, D. E. (1995). Dynamic Business Continuity Planning. Unpublished master's thesis. Port Elizabeth Technikon, Port Elizabeth, South Africa.
- Campbell, R., Danton, M., Hodgetts, V., Melamed, I. & Spagnolo, A. (n.d.). Fighting computer crime: a BSS SecureData Manual.
- Carleton, J. (2002). Small to Medium Business: The SME Experience [Online]. [Cited February 20, 2003] Available from Internet URL
<http://www.abc.net.au/rn/learning/lifelong/stories/s730137.htm>
- Crannburn Innovative Software Solutions. (Cited September 29, 2002). Custom Software Development [Online]. Available from Internet URL
<http://www.crannburn.com/Commercial/CustomDev/main.htm>
- Crimando, S. & Steinberg, J. (1997). The Disaster Human Factors Continuum. Disaster Resource Guide [Online]. [Cited 23 October, 2000] Available from Internet URL http://www.disaster-resource.com/cgi-bin/article_search.cgi?id=145
- Davenport, P. B. (1995). ISO 9000 In A Small, Vibrant Economy, With, Typically, Small To Medium Sized Businesses. SABS Bulletin, 14 (5), pp. 24-28
- DeLuca, F. (1996). Recovery Has Its Place. Contingency Planning & Management [Online]. [Cited October 19, 2002] Available from Internet URL
http://www.contingencyplanning.com/article_index.cfm?article=9
- Devargas, M. (1999). Survival is Not Compulsory: An Introduction to Business Continuity Planning. Computers & Security, 18 (1), pp. 35-46

- Dolten, N. (1996). Mitigation: Pay Now or Pay More Later. Contingency Planning & Management [Online]. [October 19, 2002] Available from Internet URL http://www.contingencyplanning.com/article_index.cfm?article=49
- Douglas, W. J. (1998). The quest for continuous operations: Data compression speeds disaster recovery. Disaster Recovery Journal [Online]. [Cited November 21, 2000] Available from Internet URL <http://www.drj.com/articles/Win98/doug.htm>
- Eckert, P. (1999). Is your DR plan ready? : Use your 20/20 vision to ensure success. Disaster Recovery Journal [Online]. [Cited November 21, 2000] Available from Internet URL <http://www.drj.com/articles/spr99/ecke.htm>
- Edwards, B. (1994). Developing a Successful Network Disaster Recovery Plan. Information management & Computer Security, 2 (3), pp. 37-42
- Edwards, B. & Cooper, J. (1995). Testing the disaster recovery plan. Information Management & Computer Security, 3 (1), p.p. 21-27
- Eloff, J. H. P., Labuschagne, L., von Solms, R. & Verschuren, J. (Eds.). (1999). Information Security Management & Small Systems Security. United States of America: Kluwer Academic Publishers
- Fisher, P. A. P. (1996). How To Conduct A Business Impact Analysis. Disaster Recovery Journal [Online]. [Cited March 7, 2002] Available from Internet URL <http://www.drj.com/articles/sum96/fish.html>
- Florendo, R., Martens, J., Middlebrooks, R., Romanyschyn, J. & Solter, M. (1998). Internet Disaster Recovery Concepts. United States of America: International Business Machines Corporation

- Frost, C. (1994). Effective Responses for Proactive Enterprises: Business Continuity Planning. Disaster Prevention and Management, 3 (1), p.p. 7-15
- Ginn, R. D. (1989). Continuity Planning: Preventing, Surviving and recovering from Disaster. Oxford: Elsevier Science Publishers Ltd.
- Glenn, J. (2002). What Is Business Continuity Planning? How Does It Differ From Disaster Recovery Planning? Disaster Recovery Journal [Online]. [Cited May 11, 2002] Available from Internet URL <http://www.drj.com/articles/win02/1501-14p.html>
- Glorioso, R. M. & Desautels, R. E. (1999). Disaster Recovery or Disaster Tolerance: The choice is yours. Disaster Recovery Journal [Online]. [Cited November 21, 2000] Available from Internet URL <http://www.drj.com/articles/spr99/glor.htm>
- Goggins, K. (1999). Contingency Planning 101. Contingency Planning & Management [Online]. [Cited November 2, 2002] Available from Internet URL http://www.contingencyplanning.com/article_index.cfm?article=176
- Gonzalez, M. & Solter, M. (1999). E-continuity: planning for e-business. Contingency Planning & Management [Online]. [Cited November 21, 2000 Available from Internet URL http://www.contingencyplanning.com/article_index.cfm?article=176
- Gordon, C. (2000). How to Cost Justify a Business Continuation Plan to Management. Disaster Recovery Journal [Online]. [Cited March 7, 2002] Available from Internet URL <http://www.drj.com/articles/spring00/1302-05.html>
- Griffin, R. W. (1990). Management (3rd ed.). Boston: Houghton Mifflin Company
- Gulley, T. (1999). Is Your Data Safe? Protecting Critical Data in a Distributed Computing Environment. Disaster Recovery Journal [Online]. [Cited 23 October, 2000] Available from Internet URL <http://www.drj.com/articles/sum99/gull.htm>

- Guttman, B. & Roback, E. (1995). An Introduction to Computer Security: The NIST Handbook. Washington: U.S. Government Printing Office
- Hagg, A. (2001). Creating a Culture of Commitment: Contingency Planning at The Home Depot. Contingency Planning & Management [Online]. [Cited November 20, 2001] http://www.contingencyplanning.com/article_index.cfm?article=355
- Halliday, S., Badenhorst, K. & von Solms, R. (1996). A business approach to effective information technology risk analysis and management. Information Management and Computer Security, 4(1), pp. 19-31
- Hassim, M. (2000). To plan or not to plan? Accountancy SA [Online]. [Cited May 11, 2002] Available from Internet URL <http://www.accountancysa.org.za/archives/1999nov/features/plan.htm>
- Hawkins, S. M., Yen, D. C. & Chou, D. C. (2000). Disaster recovery planning: a strategy for data security. Information Management and Computer Security, 8(5), pp. 222-229
- Heng, G. M. (1996). Developing a suitable business continuity planning methodology. Information Management & Computer Security, 4 (2), 11-13
- Huff, A. (1998). Building Your Team for Crisis Communications. Disaster Resource Guide [Online]. [Cited October 23, 2000] Available from Internet URL http://www.disaster-resource.com/cgi-bin/article_search.cgi?id=72
- Hurwicz, M. (2000). When Disaster Strikes (Industry Trend or Event). Network Magazine [Online]. [Cited May 11, 2002] Available from Internet URL <http://www.networkmagazine.com/article/NMG20000510S0027>
- IBM Global Services. (1999). Business Continuity: New risks, new imperatives and a

new approach. England: Carwin

IBM Global Services. (2000). Managing information technology in a new age

[Online]. [Cited October 18, 2000] Available from Internet URL
<http://www.ibm.com/services/whitepapers/gsw1178f.html>

Jackson, C. & Carey, M. (1997). Budgeting Basics. Contingency Planning & Management [Online] [Cited October 19, 2002] Available from Internet URL

http://www.contingencyplanning.com/article_index.cfm?article=62

Johnson, D.A. (1998). Managing the Recovery Planning Project: part 2. Disaster Recovery Journal [Online]. [Cited November 21, 2000] Available from Internet URL

<http://www.drj.com/articles/Win98/john.htm>

Johnson, J. (2002). Internal Auditing [Online]. [Cited October 31, 2002] Available from Internet URL

<http://cobacourses.creighton.edu/fin402/Semester%20Projects/johnson.htm>

Karakasidis, K. (1997). A project planning process for business continuity.

Information Management & Computer Security, 5 (2), pp. 72-78

Kearvell-White, B. (1996). KPMG's UK Computer Security Review 1994.

Information Management and Computer Security, 4(2), pp. 42-51

King Committee on Corporate Governance (2001). King Report On Corporate Governance

For South Africa 2001 [Online]. [Cited September 29, 2002] Available from Internet URL
<http://www.iodsa.co.za/IOD%20Draft%20King%20Report.pdf>

King, J. W. (2000). Business Continuity Planning & the highly protected risk

expanding the envelope: Planning for the entire organisation. Disaster Recovery Journal [Online]. [Cited October 23, 2000] Available from Internet URL

<http://www.drj.com/articles/win00/1301-06.html>

Koski, K. (2001). Backup and Offsite Vaulting [Online]. [Cited November 21, 2000]

Available from Internet URL <http://w3.arcusds.com/Backup%20White%20Paper.pdf>

LaPedis, R. (2001). Disaster Recovery: No Longer Enough. Disaster Recovery Journal [Online]. [Cited January 21, 2000] Available from Internet URL <http://www.drj.com/articles/sum01/1403-01p.html>

Larue, J. (2000). How Far is Really Far Enough Away? Disaster Recovery Journal [Online]. [Cited February 20, 2003] Available from Internet URL <http://www.drj.com/articles/fal00/1304-01.html>

Leiwo, J., Kajava, J. & Nesland, L. (1994). Information Security Guide-lines for End-User Computing. Agder University College: Norway

Maslen, C. (1996). Testing the plan is more important than the plan itself. Information Management & Computer Security, 4 (3), 26-29.

McAnally, P., DiMartini, B., Hakun, J., Lindman, G. & Parker, R. (2000). Real-time data availability solutions: Does your business have a need for speed? Disaster Resource Guide [Online]. [Cited May 11, 2001] Available from Internet URL http://www.disaster-resource.com/cgi-bin/article_search.cgi?id='22'

McKinney, C. C. (2000). Does your plan measure up? Contingency Planning & Management [Online]. [Cited May 11, 2001] Available from Internet URL http://www.contingencyplanning.com/article_index.cfm?article=321

Megginson, W. L. (1994). Small business management: an entrepreneurs guide to success. United States of America: R.R Donnelley & Sons Company

Moore, P. (1995). Critical elements of a disaster recovery and business/service continuity plan. Facilities, 13(9), pp. 22-27

Moore, P. (1997). How to plan for enterprise-wide business and service continuity

Disaster Resource Guide [Online]. [Cited October 15, 2000] Available from Internet URL http://www.disaster-resource.com/cgi-bin/article_search.cgi?id='48'

Morwood, G. (1998). Business continuity: awareness and training programmes.

Information Management & Computer Security, 6 (1), 28-32

Nosworthy, J. (1999). Y2K Contingency Planning: Taking BCM into the 21st Century. Computers & Security, 18 (8), 693-704

Ogorchok, J. (1998). Business continuance: beyond disaster recovery. Disaster Recovery Journal [Online]. [Cited November 21, 2000] Available from Internet URL <http://www.drj.com/articles/Win98/ogor.htm>

Paradine, T. J. (1995). Business interruption insurance: a vital ingredient in your disaster recovery plan. Information Management & Computer Security, 3 (1), pp. 9-17

Romney, M. B. (2000). Accounting information systems. New Jersey: Prentice-Hall Inc.

Rospond, K. M. (1996). Insurance...Do You Have What It Takes? Disaster Resource Guide [Online]. [Cited October 21, 2000] Available from Internet URL http://www.disaster-resource.com/cgi-bin/article_search.cgi?id=49

Rubin, H. (May/June 1999). Bracing for Zero Day. IT Pro. pp.73-76

Salemo, C. (1999). Source File: Alternate Sites. Contingency Planning & Management [Online]. [Cited November 21, 2000] Available from Internet URL http://www.contingencyplanning.com/article_index.cfm?article=219

Scheur Management Group. (1999). How Healthy Is Your Business [Online]. [Cited October 31, 2002] Available from Internet URL <http://www.scheur.com/1technology/webpage/e-commerce.nsf/webcontent/ConsultantColumnsHealthyBusiness.html>

Smith, M. & Sherwood, J. (1995). Business Continuity Planning. Computers & Security, 14 (1), 14-23

- Stallings, W. (1995). Network and Internetwork Security: Principles and Practice.
New Jersey: Prentice Hall
- Steers, R. M. & Porter, L. W. (1991). Motivation And Work Behaviour. McGraw-Hill
Book Co: Singapore
- Steinberg, J. & Saracco, D. (1998). Business Depends on People. Disaster Resource
Guide [Online]. [Cited October 17, 2001] Available: [http://www.disaster-
resource.com/cgi-bin/article_search.cgi?id=68](http://www.disaster-resource.com/cgi-bin/article_search.cgi?id=68).
- Straus, S. G., Weisband, S. P. & Wilson, J. M. (1998). Human Resource Management
Practices in the Networked Organization: Impacts of Electronic Communication
Systems. In C. L. Cooper & D. M. Rousseau (Eds.). Trends in Organizational
Behaviour. (pp. 127-154). England: John Wiley & Sons Ltd.
- Takemura, R. & Taylor, R. M. (1996). The Increasing Need For Client/Server
Contingency Planning. Disaster Resource Guide [Online]. [Cited November 21, 2000]
Available from Internet URL [http://www.disaster-resource.com/cgi-
bin/article_search.cgi?id=36](http://www.disaster-resource.com/cgi-bin/article_search.cgi?id=36)
- Turley, B. (2000). Web-Based Planning: A BCP Manager's New Best Friend!
Disaster Resource Guide [Online]. [Cited October 30, 2001] Available from Internet
URL http://www.disaster-resource.com/cgi-bin/article_search.cgi?id=12
- Tydlaska, L. (1996). What's Behind Your backup Plan. Contingency Planning &
Management [Online]. [Cited October 19, 2000] Available from Internet URL
http://www.contingencyplanning.com/article_index.cfm?article=7
- Tyson, S. & Jackson, T. (1992). The Essence of Organizational Behaviour. United
Kingdom: Prentice Hall International Ltd.
- Underwood, M. (1998). Disaster recovery services help keep operations flowing for

AS/400 systems. Disaster Recovery Journal [Online]. [Cited October 21, 2000]
Available from Internet URL <http://www.drj.com/articles/fall98/under.htm>

United States General Accounting Office. (1998). Year 2000 Computing Crisis: Business Continuity and Contingency Planning [Online]. [Cited October 23, 2000]
Available from Internet URL <http://www.gao.gov/special.pubs/ai10119.pdf>

Van Mill, S & Gliane, A. (1997). Insurance Disaster Recovery Planning: Business Income Coverage and Claims Preparation. Disaster Recovery Journal [Online]. [Cited 23 October, 2000] Available from Internet URL
<http://www.drj.com/articles/DRJezine/nov97/vanmill.htm>

Veryard Projects. (2002). Methodology [Online]. [Cited May 15, 2002]
Available from Internet URL <http://www.veryard.com/sebpc/methodology.htm>

Vistastor Corporation (2002). ROI And The Costs of Business Continuity Planning [Online]. [Cited September 29, 2002] Available from Internet URL
<http://www.vistastor.com/briefs/ROI.pdf>

von Solms, R (1999). Information security management: why standards are important. Information Management and Computer Security, 7(1), pp. 50-57

Weems, T. L. (1999) Business Continuity Planning-for the rest of us. Disaster Recovery Journal [Online]. [Cited October 23, 2000] Available from Internet URL
<http://www.drj.com/articles/fall99/weem.htm>

Wilson, B. (2000). Business Continuity Planning: A Necessity In The New E-Commerce Era. Disaster Recovery Journal [Online]. [Cited October 21, 2000]
Available from Internet URL <http://www.drj.com/articles/fal00/1304-02.htm>

Wold, G.H. (1996). Some Techniques For Business Impact Analysis. Disaster Recovery Journal [Online]. [Cited March 7, 2002] Available from Internet URL
<http://www.drj.com/articles/fal96/wold.html>

Wold, G. H. & Vick, T. L. (2000). The Recovery Team Planning Approach. Disaster Recovery Journal [Online]. [Cited 21 October, 2000] Available from Internet URL <http://www.drj.com/articles/fal00/1304-04.html>

Wrobel, L. A. (Cited October 17, 2000). Components Of A Successful LAN Disaster Recovery Plan. Disaster Resource Guide [Online]. Available from Internet URL http://www.disaster-resource.com/articles/components_success_wrobel.shtml

Yngström, L. & Carlsen, J. (Eds.). (1997). Information Security in Research and Business. London: Chapman & Hall

ANNEXURE A

BCP Cyclic

System Documentation

Contents

1. BCP Cyclic: An Introduction.....	173
1.1. Introduction.....	173
1.2. Programming language	173
2. Database Design	174
2.1. Introduction	174
2.2. The selected database engine.....	174
2.3. Database design	174
2.4. Database tables	175
2.4.1. AltSiteDetails Table	177
2.4.2. AltSites Table.....	177
2.4.3. ChosenTasks Table	178
2.4.4. CompTest Table.....	178
2.4.5. ContinuityEmp Table	179
2.4.6. DetProcedures Table	179
2.4.7. EmergencyContacts Table	180
2.4.8. EmergencyProc Table	180
2.4.9. EmpHoldTasks Table	181
2.4.10. Employees Table	182
2.4.11. EmpTasks Table.....	182
2.4.12. EmResources Table.....	183
2.4.13. FullTest Table	183
2.4.14. HardSoft Table.....	184
2.4.15. Hardware Table.....	184
2.4.16. HoldStrat Table	185
2.4.17. InsuranceCoverage Table	185
2.4.18. InsuranceDetails Table	186
2.4.19. IntTest Table	186
2.4.20. InvocProc Table	187

2.4.21. MaintComm Table	187
2.4.22. PlanObj Table	188
2.4.23. Plans Table.....	188
2.4.24. ProcDocs Table.....	189
2.4.25. ProcEmp Table.....	189
2.4.26. Processes Table	190
2.4.27. ProcessTasks Table	191
2.4.28. ProcFiles Table	191
2.4.29. ProcHard Table	191
2.4.30. ProcSoft Table.....	192
2.4.31. PublicRel Table.....	192
2.4.32. Scenarios Table.....	193
2.4.33. Software Table.....	193
2.4.34. Tasks Table	194
2.4.35. TeamEmp Table.....	194
2.4.36. Teams Table.....	195
2.4.37. Vendors Table.....	195
3. Business Process Criticality Calculation.....	196
3.1. Introduction	196
3.2. Calculating criticality.....	196

1. BCP Cyclic: An Introduction

1.1. Introduction

The BCP Cyclic prototype is an implementation of a Business Continuity Planning (BCP) methodology. The methodology is a result of a study of various other existing continuity planning methodologies and their shortcomings. Furthermore, the prototype not only implements the above-mentioned methodology, but does this in four separate cycles. The application in question, therefore, allows a user to build a business continuity plan in four relatively unique phases.

BCP Cyclic makes use of an information gathering process to collect organisational information required to produce a detailed business continuity plan. It then makes use of this information to make calculations, which would normally have been done manually or make suggestions to what recovery and continuity options are to be chosen. This will assist a user to produce a more effective and efficient business continuity plan.

This documentation will discuss technical issues and decisions that have been made in order to develop this prototype. It will furthermore discuss how the methodology mentioned in the previous paragraph has been implemented in a software package.

1.2. Programming language

For this specific package, the programming language found to be most appropriate was Microsoft Visual Basic. Firstly, it was found that interface development occurred much more rapidly and this is very important, specifically for the application in question. The BCP cyclic application, and especially the information-gathering wizard, consists of a relatively large number of screens, each containing a variety of information inputs. The design of these screens, therefore, needs to be completed swiftly.

Firstly, screen design forms a minor part of the entire application design. Consequently, one would rather spend more time on screen functionality than its design. Secondly, to ensure that application development is completed in the least amount of time, it is best to

save time wherever possible. A good way to accomplish this is through rapid interface development, leaving more time for the functionality aspect of the application.

2. Database Design

2.1. Introduction

The BCP Cyclic application, by nature, gathers large amounts of organisational information. For this reason a storage mechanism is a necessity. Such a mechanism will need to be accessed frequently either to access stored information or store gathered information. Stored information needs to be partitioned in a logical manner to allow ease of access. A relational database would serve this purpose well. This database's design and various other issues will be discussed below.

2.2. The selected database engine

The database engine chosen for the BCP Cyclic database is Microsoft Access 2000. This database engine provides a simple interface for designing a database as required by BCP Cyclic. A large number of relational tables is required by the application in question and MS Access provides a quick and easy way to create such tables. The amount of information to be stored is also not that great and the chosen engine would, therefore, be more than adequate. The amount of characters to be stored in any of the table fields will also never exceed 255 characters, which makes the chosen database engine even more appropriate. Lastly, the programming language used supports database access for the chosen database very well.

2.3. Database design

The BCP Cyclic information storage database design is based closely on the BCP methodology chosen for this application. This methodology is depicted in **figure 2.1**. This methodology firstly collects important planning information during the *Project Planning* phase. After this, business processes are examined and their organisational impact is determined during the *Business Impact Analysis* phase. Once these two exercises have

been completed, strategies for recovery and business continuation are identified during the *Business Continuity Strategies* phase. These strategies are furthermore implemented during the *Continuity Strategies Implementation* phase. After this, the *Testing* and *Maintenance* phases follows. The creation of tables will be discussed in more detail in the following section.

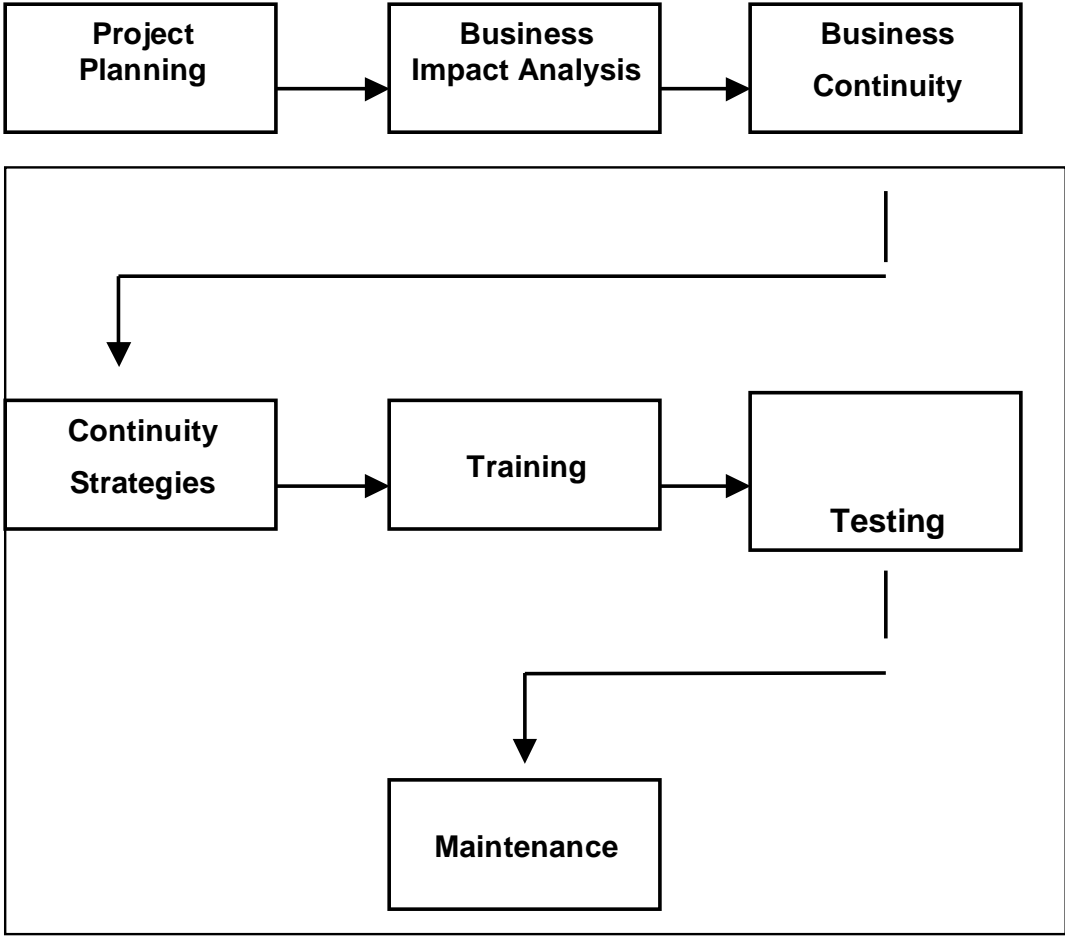


Figure A.2.1: The BCP Cyclic methodology

2.4. Database Tables

The design of database tables following the methodology depicted in **figure 2.1** will be discussed below. A representation of the relationships between the various tables can be seen in **figure 2.2**. Below follows a description of each table and the fields created for each.

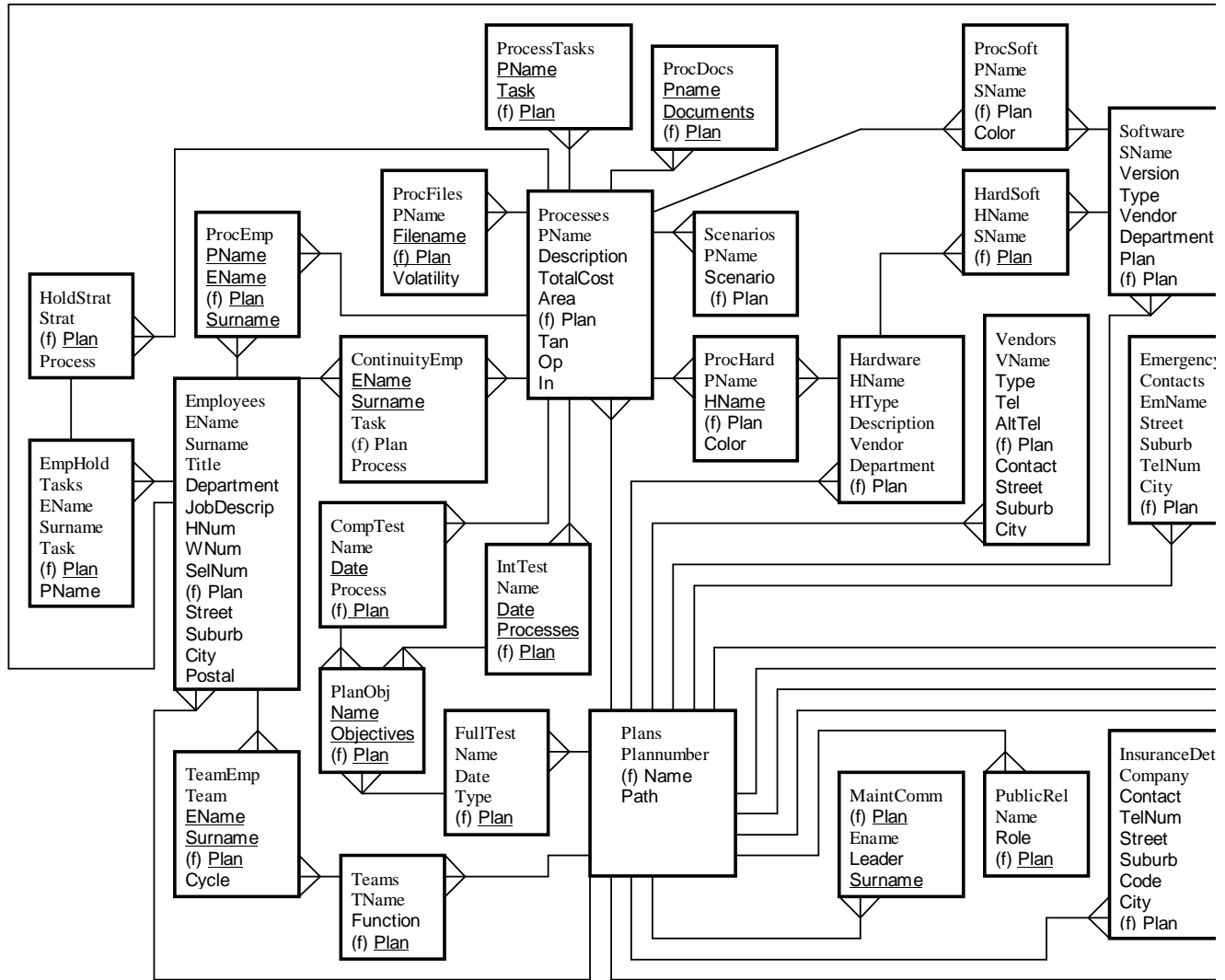


Figure A.2.2: BCP Cyclic database design

2.4.1. AltSiteDetails Table

The purpose of this table is to store information relating to the chosen alternate data processing strategy. It stores mainly location details and also contact details in case of a vendor based solution.

Fields:

- o Vendor : This field contains the vendor (if applicable) that provides the alternate processing solution
- o Contact : This field contains either the employee responsible for the alternate processing solution or the vendor contact person
- o Tel : This field contains the contact number for the contact person
- o Street : This field contains the alternate processing solution street address
- o Suburb : This field contains the alternate processing solution suburb
- o SiteTel : This field contains the alternate processing solution contact number
- o Plan : This field contains the name of the organisation or plan that this alternate processing solution applies to.

2.4.2. AltSites Table

The purpose of this table is to store the chosen alternate data processing strategy for each plan within the database.

Fields:

- o Alternatives : This field contains the chosen alternative processing solution
- o Plan : This field contains the name of the organisation or plan that this alternate processing solution applies to.

2.4.3. ChosenTasks Table

The purpose of this table is to store the IT infrastructure recovery tasks for each Business Continuity Planning cycle. The tasks in this table are divided into suggested and additional user added tasks. They are furthermore divided into those tasks that have been selected for inclusion in the plan and those that are not.

Fields:

- o MTasks : This field contains the major recovery tasks for a given plan
- o Plan : This field contains the plan name to which the major tasks are applicable.
- o Cycle : This field contains the cycle to which the major tasks are applicable
- o Checked : This field indicates whether a major task is to be included in a business continuity plan
- o Suggested : This field is used to indicate whether a major task is suggested by the BCP Cyclic application or additionally added

2.4.4. CompTest Table

The purpose of this table is to store the scheduled component tests for each business continuity plan within the database. Important information stored includes test dates and processes involved.

Fields:

- o Name : This field contains the name of the component test
- o Date : This field contains the date that each component test is to be performed
- o Process : This field contains the name of the process that the test is applicable to
- o Plan : This field contains the name of the plan for which the component test is scheduled

2.4.5. ContinuityEmp Table

The purpose of this table is to store the tasks that ensure process continuity for each process along with the employees to whom these tasks have been assigned. This table shows exactly what each employee's responsibility is for each process.

Fields:

- o EName : This field contains the name of the employee involved in ensuring process continuity
- o Surname : This field contains the surname of the employee involved in ensuring process continuity
- o Task : This field contains the task to be completed to ensure process continuity
- o Plan : This field contains the name of the plan for which the continuity procedures are identified
- o Process : This field contains the name of the business process for which the continuity procedures are identified

2.4.6. DetProcedures Table

The purpose of this table is to store the detailed IT infrastructure recovery procedures for each of the identified major tasks. The table is also used to store the cycles to which each task is applicable.

Fields:

- o MTask : This field contains the major IT infrastructure recovery task for a specific plan
- o Dtask : This field contains the detailed IT infrastructure recovery task for a specific plan
- o Plan : This field contains the name of the plan the detailed recovery tasks are applicable to
- o Cycle : This field contains the cycle that the detailed recovery tasks are applicable to

2.4.7. EmergencyContacts Table

The purpose of this table is to store the contact details for a variety of emergency services possibly required by each plan within the database.

Fields:

- o EmName : This field contains the name of type of emergency service provider as required by organisations
- o Street : This field contains the street address of the emergency service provider
- o Suburb : This field contains the suburb of the emergency service provider
- o TelNum : This field contains the contact number of the emergency service provider
- o City : This field contains the city where the emergency service provider is located
- o Plan : This field contains the plan name for which the emergency service providers' details are stored

2.4.8. EmergencyProc Table

The purpose of this table is to store the emergency response and notification procedures for each of the plans within the database. The procedures are divided into three different categories based on the severity of the disaster.

Fields:

- o Procedures : This field contains the emergency response procedures identified for each plan
- o Plan : This field contains the name of the plan to which these procedures apply
- o Number : This field contains the order of emergency response procedures
- o Condition : This field contains the condition type with which procedures are classified

2.4.9. EmpHoldTasks Table

The purpose of this table is to store the pre-disaster procedures that need to be completed in order to ensure business process continuity in a disaster situation. The employee details for those employees that will perform these procedures and what procedures each will perform are also stored.

Fields:

- o EName : This field contains the name of the employee to complete a specific holding strategy task
- o Surname : This field contains the surname of the employee to complete a specific holding strategy task
- o Task : This field contains the various holding strategy tasks that need to be completed for a specific business process
- o Plan : This field contains the name of the plan that the holding strategy tasks have been identified for
- o PName : This field contains the names of business processes for which holding strategy tasks have been identified

2.4.10. Employees Table

The purpose of this table is to store a variety of details for all organisational employees for a specific business continuity plan.

Fields:

- o EName : This field contains the organisational employees' names
- o Surname : This field contains the organisational employees' surnames
- o Title : This field contains the organisational employees' job titles
- o Department : This field contains the organisational employees' departments
- o JobDescrip : This field contains a description of the function an employee performs in the organisation
- o Hnum : This field contains the organisational employees' home contact number
- o Wnum : This field contains the organisational employees' work contact number
- o SelNum : This field contains the organisational employees' mobile phone number
- o Plan : This field contains the name of the plan or organisation this employee belongs to
- o Street : This field contains the organisational employees' street address
- o Suburb : This field contains the organisational employees' suburb
- o City : This field contains the organisational employees' city or town of residence

- o Postal : This field contains the organisational employees' postal code

2.4.11. EmpTasks Table

The purpose of this table is to store the various employees involved in IT infrastructure recovery as well as the various recovery tasks that they need to complete.

Fields:

- o EName : This field contains the name of the employee to whom recovery tasks are assigned
- o Surname : This field contains the surname of the employee to whom recovery tasks are assigned
- o Task : This field contains the recovery tasks assigned to the various employees
- o Plan : This field contains the name of the plan that the recovery task apply to
- o Cycle : This field contains the cycle that the recovery tasks applies to

2.4.12. EmResources Table

The purpose of this table is to store the various required emergency resources that will be used during disaster situations.

Fields:

- o Resource : This field contains the name and type of the emergency resource
- o Plan : This field contains the name of the plan for which emergency resources have been identified
- o Location : This field contains the storage location of each resource

2.4.13. FullTest Table

The purpose of this table is to store the scheduled full tests (simulated and live) for each business continuity plan within the database.

Fields:

- o Name : This field contains the name assigned to the full test in question
- o Date : This field contains the date a specific full test has been scheduled for
- o Type : This field contains the type of full test that has been scheduled
- o Plan : This field contains the name of the plan that each full test has been scheduled for

2.4.14. HardSoft Table

The purpose of this table is to store the software (if applicable) required by certain organisational hardware.

Fields:

- o HName : This field contains the name of the hardware item in question
- o SName : This field contains the name of the software that each hardware item is dependant on or utilises
- o Plan : This field contains the name of the plan to which the hardware and software are assigned

2.4.15. Hardware Table

The purpose of this table is to store a variety of details for all organisational hardware for a specific business continuity plan.

Fields:

- o HName : This field contains the name of the hardware item to be stored
- o HType : This field contains a type or category to which each hardware item belongs
- o Description : This field contains a brief description of each hardware item
- o Vendor : This field contains the name of the vendor or supplier of each hardware item

- o Department : This field contains the name of the department that uses each item
- o Plan : This field contains the name of the plan for which hardware items have been recorded

2.4.16. HoldStrat Table

The purpose of this table is to store the pre-disaster procedures that need to be completed in order to ensure business process continuity in a disaster situation.

Fields:

- o Strat : This field contains identified user holding strategies for each process
- o Plan : This field contains the name of the plan that strategies have been identified for
- o Process : This field contains the name of the specific process for which strategies have been identified

2.4.17. InsuranceCoverage Table

The purpose of this table is to store the coverage given by each stored insurance policy and for each stored organisation.

Fields:

- o Coverage : This field contains the name of a coverage a specific insurance policy caters for
- o Plan : This field contains the name of the plan to which an identified coverage applies

- o Company : This field contains the name of an insurance company that issued the policy having a specific coverage

2.4.18. InsuranceDetails Table

The purpose of this table is to store all the necessary details for every insurance policy and company for every organisation within the database.

Fields:

- o Company : This field contains the name of an insurance company providing a specific policy
- o Contact : This field contains the name of the individual to be contacted with regard to policy queries
- o TelNum : This field contains the contact number of the above mentioned individual or company
- o Street : This field contains the street address of the insurance company providing the service
- o Suburb : This field contains the suburb of the insurance company providing the service
- o Code : This field contains the postal code of the insurance company providing the service
- o City : This field contains the city of the insurance company providing the service
- o Plan : This field contains the name of the plan to which the insurance policy applies

2.4.19. IntTest Table

The purpose of this table is to store the scheduled component tests for each business continuity plan within the database. Important information stored includes test dates and processes involved.

Fields:

- o Name : This field contains the name of the scheduled integrated test
- o Date : This field contains the date that an integrated test has been scheduled for
- o Processes : This field contains then names of business processes each test involves
- o Plan : This field contains the name of the plan that each integrated test applies to

2.4.20. InvocProc Table

The purpose of this table is to store the conditions for plan activation, i.e. when will what actions be taken. Conditions are categorised into three main types of conditions that are determined by the severity of the disaster.

Fields:

- o Condition : This field contains the conditions or categories of plan activation
- o Procedure : This field contains the procedures to be followed under certain conditions

- o Plan : This field contains the name of the plan to which the procedures and conditions apply

2.4.21. MaintComm Table

The purpose of this table is to store the names and details of all those employees involved in some way in the maintenance process of a business continuity plan.

Fields:

- o Plan : This field contains the name of the plan for which a maintenance committee is identified
- o EName : This field contains the name of an employee belonging to the maintenance committee
- o Leader : This field indicates whether an employee is in charge of the maintenance process
- o Surname : This field contains the surname of an employee belonging to the maintenance committee

2.4.22. PlanObj Table

The purpose of this table is to store the objectives for tests that are conducted to determine plan efficiency and effectiveness. This tables store the objectives for all three types of tests (Component, Integrated and Full tests)

Fields:

- o Name : This field contains the name of the test to which objectives apply
- o Objectives : This field contains the objectives assigned to each test
- o Plan : This field contains the name of the plan to which objectives and tests apply

2.4.23. Plans Table

The purpose of this table is to store all existing business continuity plans and each plan's cyclic progress.

Fields:

- o Plan : This field contains the name of the plan for which cyclic progress is stored
- o Cycle : This field contains the current cycle for the plan listed in the above field

2.4.24. ProcDocs Table

The purpose of this table is to store all the important documents required to ensure process continuity.

Fields:

- o PName : This field contains the names of the business processes for which important documents are listed
- o Documents : This field contains a listing of important documents for ensuring business process continuity
- o Plan : This field contains the name of the plan for which documents are listed

2.4.25. ProcEmp Table

The purpose of this table is to store details of all employees involved in every stored organisation's business processes.

Fields:

- o PName : This field contains the names of the business processes for which employees are listed
- o EName : This field contains the names of employees involved in each business process
- o Plan : This field contains the name of the plan for which employees and processes are listed
- o Surname : This field contains the surnames of employees involved in each business process

2.4.26. Processes Table

The purpose of this table is to store important details for all stored organisations' business processes.

Fields:

- o PName : This field contains the names of business processes listed for each plan
- o Description : This field contains a brief description of all business processes
- o Totalcost : This field contains a calculated value based on the average of tangible, intangible and operational costs
- o MAPD : This field contains a value indicating the maximum allowable recovery time for each process
- o Area : This field contains a value stating which area on a graph used to calculate process criticality the process falls under
- o Plan : This field contains the name of the plan each business process is listed for
- o Tan : This field contains a value indicating tangible costs for business processes
- o Op : This field contains a value indicating operational costs for business processes
- o In : This field contains a value indicating intangible costs for business processes

2.4.27. ProcessTasks Table

The purpose of this table is to store the procedures that will ensure business process continuity for each of the stored organisations' business process.

Fields:

- o PName : This field contains the name of the business process to which continuity tasks listed in this table are applicable
- o Task : This field contains tasks that will ensure business process continuity when disaster has struck
- o Plan : This field contains the name of the plan to which listed tasks apply

2.4.28. ProcFiles Table

The purpose of this table is to store important files used by the various stored business process that are required to ensure process continuity.

Fields:

- o PName : This field contains the name of the process for which files are listed in the *Filename* field
- o Filename : This field contains the names of files listed for each process that are required for business continuity
- o Plan : This field contains the name of the plan for which files and processes are listed
- o Volatility : This field contains an estimate of how often specific files change and needs to be backed up

2.4.29. ProcHard Table

The purpose of this table is to store all the important hardware utilised by the various stored business process that are required to ensure process continuity.

Fields:

- o PName : This field contains the name of business processes for which hardware is listed in the field below
- o HName : This field contains the names of hardware items listed for each business process
- o Plan : This field contains the name of the plan business processes and their hardware are listed for
- o Color : This field contains a value categorizing the importance of a specific hardware item for each process

2.4.30. ProcSoft Table

The purpose of this table is to store all the important software utilised by the various stored business process that are required to ensure process continuity.

Fields:

- o PName : This field contains the name of business processes for which software is listed in the field below
- o SName : This field contains the names of software items listed for each business process
- o Plan : This field contains the name of the plan business processes and their software are listed for

- o Color : This field contains a value categorizing the importance of a specific software item for each process

2.4.31. PublicRel Table

The purpose of this table is to store all employees involved in ensuring that public relations are conducted appropriately.

Fields:

- o Name : This field contains the names of employees involved in public relation for the organisation
- o Role : This field contains the role employees listed above in the public relations process
- o Plan : This field contains the name of the plan for which employees and roles are listed in the above fields

2.4.32. Scenarios Table

The purpose of this table is to store a collection of disaster scenarios for each identified business process.

Fields:

- o PName : This field contains the name of business process for which disaster scenarios are listed in the next field
- o Scenario : This field contains a listing of disaster scenarios for each process
- o Plan : This field contains the name of the plan for which scenarios are listed

2.4.33. Software Table

The purpose of this table is to store all the necessary details for software as used by the various stored organisations and their business continuity plans.

Fields:

- o SName : This field contains the name of the software item to be stored
- o Version : This field contains the version of each software item
- o Type : This field contains the type or category the software item belongs to
- o Vendor : This field contains the name of the vendor that supplied the software
- o Department : This field contains the name of the department using the software
- o Plan : This field contains the name of the plan for which the software is listed

2.4.34. Tasks Table

The purpose of this table is to store all suggested IT infrastructure recovery tasks that can be applied to and selected for all business continuity plans.

Fields:

- o Task : This field contains IT infrastructure recovery tasks
- o Cycle : This field contains the cycle for which each task is intended

2.4.35. TeamEmp Table

The purpose of this table is to store teams and the employees that belong to them for each organisation and plan.

Fields:

- o Team : This field contains the name of a specific recovery team
- o EName : This field contains the names of employees belonging to a team
- o Surname : This field contains the surname of employees belonging to a team
- o Plan : This field contains the name of the plan for which teams and employees are listed
- o Cycle : This field contains the cycle in which teams are utilised

2.4.36. Teams Table

The purpose of this table is to store all identified teams for those organisations stored in the database.

Fields:

- o TName : This field contains the name of an identified recovery team
- o Function : This field contains a brief description of each team's function
- o Plan : This field contains the name of the plan for which teams are identified

2.4.37. Vendors Table

The purpose of this table is to store a collection of vendors and suppliers for the hardware and software that the organisational business processes are dependant on.

Fields:

- o VName : This field contains the name of a vendor or supplier to an organisation
- o Type : This field contains the type of vendor, e.g. hardware or software
- o Tel : This field contains a contact number for a vendor
- o AltTel : This field contains a alternate contact number for a vendor
- o Plan : This field contains the name of the plan for which vendors have been listed
- o Contact : This field contains the name of a contact person representing the vendor
- o Street : This field contains the vendor's street address
- o Suburb : This field contains the vendors suburb
- o City : This field contains the vendor's city
- o Postal : This field contains the vendor's postal code

3. Business Process Criticality Calculation

3.1. Introduction

When business processes have been identified and their criticality factors, i.e. how their unavailability would affect the organisation, have been determined, the overall process criticality needs to be calculated. The BCP Cyclic application performs this function at the end of the Business Impact Analysis phase once all business process information has been entered.

Once calculated, the BCP Cyclic application produces an impact analysis report based on calculations. The following section will discuss the method used to calculate business process criticality.

3.2. Calculating criticality

Time tolerance for each function is not enough to determine the recovery order for organisational processes. Therefore, values have to be established for costs that have an impact on business processes, such as tangible, intangible and operational costs. The table depicted below could be used to determine their impact value. BCP Cyclic makes use of these values to determine the tangible and operational costs for each process by assigning such a value as soon as the user indicates it.

Description	Value
Very Low Impact	1
Noticeable Impact	2
Significant Impact	3
Severe Impact	4
Very High Impact	5
Critical Impact	6

Table A.3.1: Tangible and Operational Cost Values

Intangible costs are difficult to assign a value to. For this reason, a table with impact ranking is once again used to identify the intangible cost for each business process. The scale of one to six is used again to keep the method for determining impact costs standard. The following table could, therefore, be used and BCP Cyclic makes use of such a table.

High	-----	Medium	-----	Low	
6	5	4	3	2	1

Table A.3.2: Intangible Cost Values

Once all three values have been identified, BCP Cyclic calculates an average ranking which is simply the average of the three combined impact costs.

Finally, the Recovery Time Objective (RTO) value for each process is used. The table below is used to determine a ranking for each business function.

Time Period	Value
0 to 6 hours	1
6+ to 48 hours	2
2 to 5 days	3
5 days to 2 weeks	4
2 weeks to 2 months	5
2 months to 2 months +	6

Table A.3.3: RTO Values

The two identified values (average cost and RTO values) can now be used to determine process priority by plotting each process on the Time tolerance and cost of impact graph, as depicted in figure 3.1. When all identified business processes have been incorporated into the graph, their position on the graph can be used to determine their various priorities. The graph is divided into sectors ranging from 1 to 6.

The most critical processes are those found in sector 6 and the least important processes are found in sector 1 on the graph. BCP Cyclic makes use of the graph concept to calculate overall process criticality. The application calculates in which area of the graph a process would be placed by means of if statements examining each process's combined average cost and RTO value.

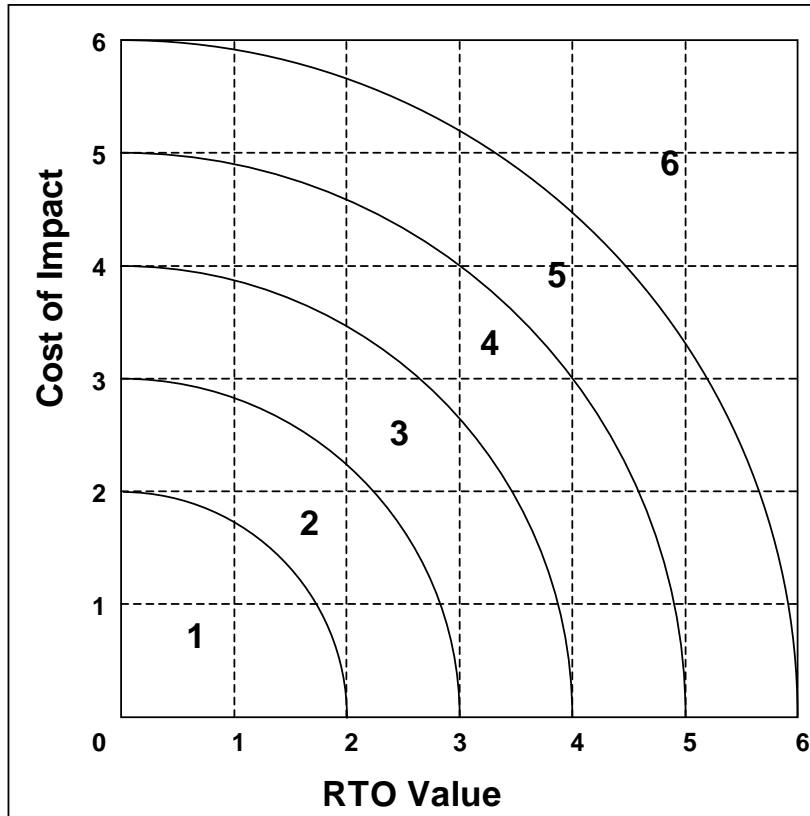


Figure A.3.1: RTO value and cost of impact graph

ANNEXURE B

BCP Cyclic

User Manual

Contents

2. Introduction to BCP Cyclic.....	202
3.3. Introduction.....	202
3.4. Disclaimer.....	202
3.5. Installation.....	203
3.6. System Requirements.....	203
4. The BCP Cyclic User Interface.....	204
4.1. Introduction.....	204
4.2. The Cyclic progress indicator.....	204
4.3. The Information Gathering Wizard progress indicator.....	205
5. Using BCP Cyclic.....	206
5.1. Getting started.....	206
5.1.1. Continuing an existing plan.....	206
5.1.2. Starting a new plan.....	207
5.2. The Information Gathering Wizard.....	207
5.2.1. The Backup Cycle (Cycle 1).....	208
5.2.1.1. Project Planning.....	208
5.2.1.2. Business Impact Analysis.....	210
5.2.1.3. Business Continuity Strategies.....	216
5.2.1.4. Continuity Strategies Implementation.....	217
5.2.1.5. Testing.....	221
5.2.1.6. Maintenance.....	223
5.2.2. The Disaster Recovery Cycle (Cycle 2).....	224
5.2.2.1. Business Continuity Strategies.....	225
5.2.2.2. Continuity Strategy Implementation.....	226

5.2.3.	The Contingency Planning Cycle (Cycle 3)	227
5.2.3.1.	Business Continuity Strategies.....	228
5.2.3.2.	Continuity Strategy Implementation	229
5.2.4.	The Business Continuity Planning Cycle (Cycle 4)	230
5.2.4.1.	Business Continuity Strategies.....	230
5.2.4.2.	Continuity Strategy Implementation	232
5.3.	The BCP Cyclic Menu and Toolbar Structure.....	232
5.3.1.	The File menu	233
5.3.2.	The View menu	234
5.3.3.	The Planning menu.....	234
5.3.4.	The BIA menu.....	234
5.3.5.	The Strategies menu	235
5.3.6.	The Implementation menu	235
5.3.7.	The Testing menu.....	236
5.3.8.	The Maintenance menu	236
5.3.9.	The Reports menu	237



1. Introduction to BCP Cyclic

1.1 Introduction

The majority of organisations today realise that they cannot function without the continued availability of their information technology resources. As they become more dependent on continuous availability of their information, they have to take measures to ensure that business continues as usual following some disaster or event. No organisation is immune to the effect of disasters and these disasters might prove fatal to its survival. They must not only ensure that their IT infrastructure can be easily recovered, but also that business can continue as usual in the wake of disaster.

Establishing procedures to ensure swift IT recovery and business continuity requires the implementation of a suitable Business Continuity Planning (BCP) methodology. The BCP Cyclic application provides the facility to construct a business continuity plan based on an effective BCP methodology.

BCP Cyclic simplifies methodology implementation by partitioning the gathering of organisational information into four different cycles. Once each cycle is completed, the BCP Cyclic application can produce a plan based on the information gathered during a specific cycle. This approach simplifies the once off approach taken by traditional BCP methodologies.

1.2 Disclaimer

The BCP Cyclic application aims to produce an effective and complete business continuity plan based on an extensive information gathering segment. It is especially suited for small to medium sized organisations to provide a means to construct a business continuity plan with a limited amount of resources. Although larger companies may make use of the software, it is generally not recommended, as the system was not designed for this purpose.

Furthermore, the BCP Cyclic application is still in a prototype stage and the plans produced by it should at present be regarded as a guideline to ensure business continuity and recovery.

1.3 Installation

The BCP Cyclic package is a standalone application and can be installed on any Microsoft Windows based machine. No installation problems should exist seeing that all required components are included in the installation package. To completely install the BCP Cyclic application and all of its components on your machine, complete the following steps:

1. Turn on your computer, allowing windows to start
2. Insert the BCP Cyclic installation CD
3. Click on the *Start* button and select the *Run* option
4. Click on *Browse*
5. Navigate to the CD-ROM drive where the CD was inserted
6. Double Click on Setup.exe
7. Follow the setup instructions

Once installation is complete, click on *Start* and select BCP Cyclic from the Windows programs menu.

1.4 System Requirements

In order to function correctly, a system running the BCP Cyclic application must have the following minimum system requirements:

- Microsoft Windows 95 or higher
- 16 megabytes of memory or higher
- At least 10 megabytes of hard disk space
- A screen resolution of 800x600 pixels or higher
- A CD ROM drive



2. The BCP Cyclic User Interface

2.1 Introduction

The BCP Cyclic application provides the user with the ability to navigate a variety of information gathering screens in order to produce a detailed business continuity plan. The following sections will, therefore, discuss the techniques utilised to indicate progress within the application.

2.2 The Cyclic progress indicator

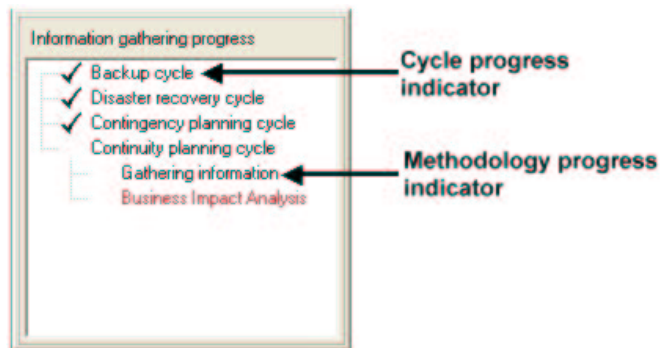


Figure B.2.1: The Cyclic Progress Indicator Window

The cyclic progress indicator is used to display exactly with which cycle one is currently busy. Along with this it also displays each cycle's current methodology phase and current methodology step.

- **Cycle progress indicator** – This is used to indicate which cycle is the current cycle. A completed cycle is indicated by means of an ✓ image alongside the appropriate item.
- **Methodology progress indicator** - This is used to indicate the current methodology phase for each cycle, as well as the current methodology step for each phase. Completed phases and steps are indicated by means of an ✓ image alongside the appropriate item.

2.3 The Information Gathering Wizard progress indicator

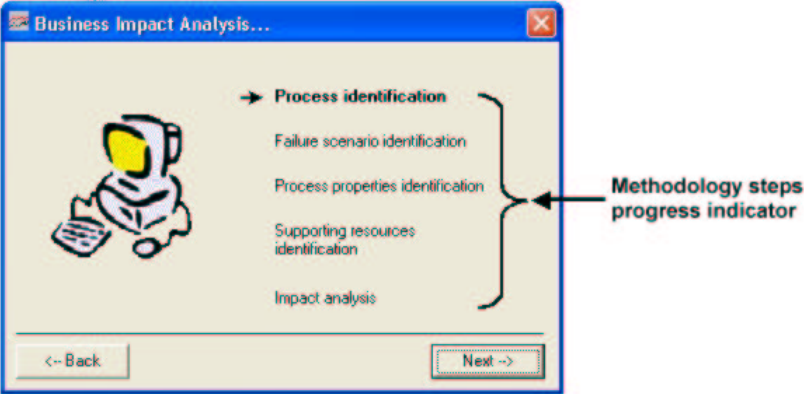


Figure B.2.2: The Information Gathering Wizard Progress Indicator

The purpose of the information-gathering wizard progress indicator is to continuously, throughout the information gathering exercise, inform you, the user, of the progress each information-gathering phase. This is done by providing a list of the various steps of each phase as seen in **figure B.2.2**. The current step is indicated by means of an ← image next to it. Once completed, the ← image is replaced with a ✓.



3. Using BCP Cyclic

3.1 Getting started

When starting the BCP Cyclic application you, the user, will be greeted by a plan commencement screen as seen in **figure B.3.1**. This screen will give you the option to start a new plan or continue an existing plan.

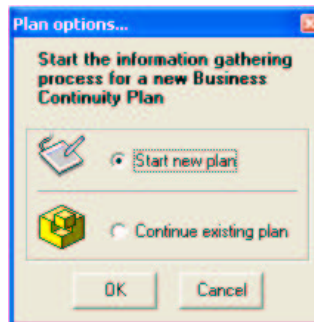


Figure B.3.1: The Plan options screen

3.1.1 Continuing an existing plan

A plan, for which one or more cycles have been completed, can be continued by selecting the *Continue existing plan* option and then clicking the button. This will display a list of existing plans. A specific plan can now be selected from the list and once selected, the button must be clicked.

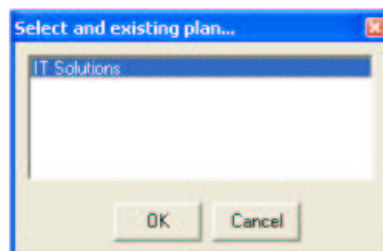


Figure B.3.2: Selecting an existing plan

Once this is done, the first screen of the Information Gathering Wizard will be displayed. The wizard will be discussed in more detail in subsequent sections.

3.1.2 Starting a new plan

If the *Start new plan* option is selected, clicking the button will result in the first screen of the information gathering wizard to be displayed. This screen can be seen in **figure B.3.3**.

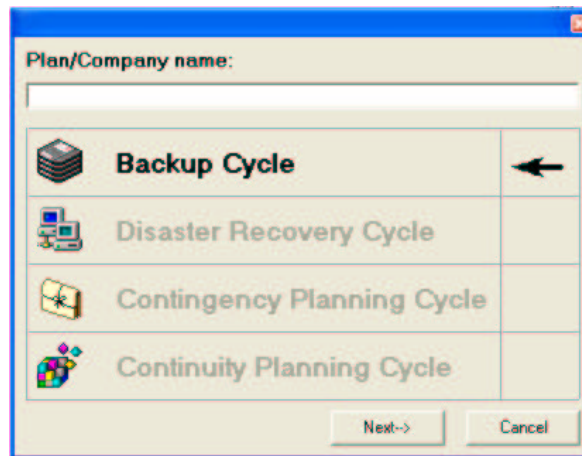


Figure B.3.3: The information-gathering wizard

The purpose of this screen is to display cyclic progress prior to conducting an information gathering exercise for a certain cycle. Those cycles that are completed will be indicated by a ✓ image alongside the completed cycle. The current cycle will be indicated by an ← image alongside it. To continue, the button must be clicked. This will start the information gathering process for the cycle indicated by ←.

3.2 The Information Gathering Wizard

The information-gathering wizard will collect the required BCP information in seven different phases. The seven phases that each cycle consists of can be seen in **figure B.3.1**. These phases will be completed for each cycle, but the steps that will be completed for each phase will differ from one cycle to the next. These steps will be discussed below.

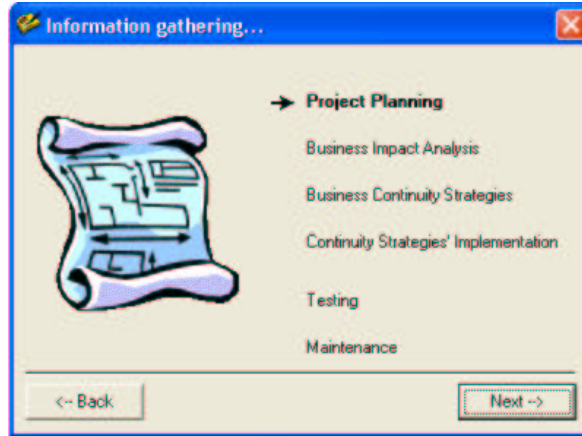


Figure B.3.4: The main progress indicator for the information-gathering wizard

3.2.1 The Backup Cycle (Cycle 1)

3.2.1.1 Project Planning

The first phase in the Backup Cycle is the **Project Planning** phase and this phase involves the collection of miscellaneous organisational information. The steps for this phase can be seen in **figure B.3.5**.

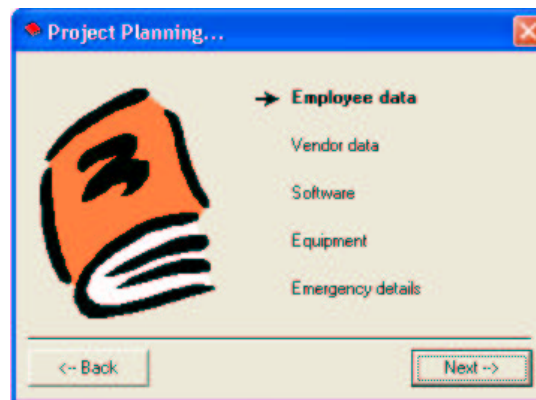


Figure B.3.5: The Project Planning wizard

All steps within the **Project Planning** phase will be completed for the first cycle and can be completed for subsequent cycles as well if desired. An option to omit this phase in subsequent cycles is given by means of a message box as can be seen in **figure B.3.6**.

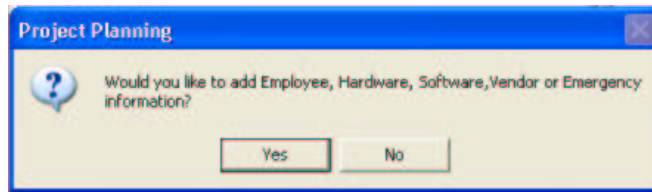


Figure B.3.6: A Project Planning message box for cycles 2, 3 and 4

○ **Adding/ Editing/ Deleting Employee, Hardware, Software and Vendor details**

Operations on Employee, Hardware, Software and Vendor details can all be done through an identical screen. This screen, as seen in **figure B.3.7**, displays a list of the item in question. In the figure, a list of Software is shown. In the case of hardware, employees etc., the software list will just be replaced by the appropriate details.

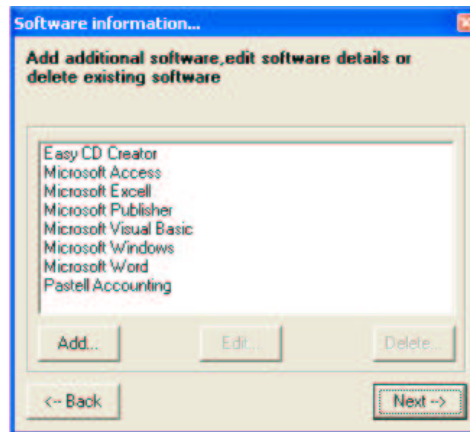


Figure B.3.7: Multi purpose list screen for Project Planning

To add an item to the list, or edit or delete an existing item, select the item from the list. Note that the **Edit...** and **Delete...** buttons are disabled. This is because none of the list items is currently selected and this is required to perform these two operations. When the **Add...** button is clicked, a data entry screen, similar to that in **figure B.3.8**, will be shown. The type of screen depends on the type of list displayed, i.e. an employee listing will require an employee information data capture screen etc.

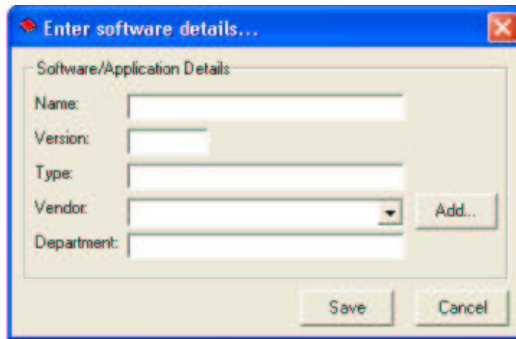


Figure B.3.8: A software details data capture screen

- **Adding/ Editing emergency details**

This operation entails entering contact details to be accessed in case of emergency. Details include Medical, Fire, Security and Law enforcement details. **Figure B.3.9** shows the emergency details information-gathering screen.

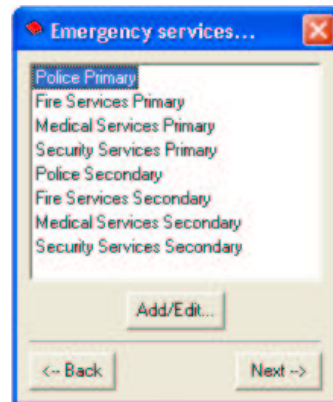


Figure B.3.9: Emergency details information gathering screen

To add or edit a certain entry, first highlight it and then click the **Add/Edit...** button. This will display the data capture screen for the specific highlighted item.

3.2.1.2 Business Impact Analysis

The second Backup Cycle phase is the **Business Impact Analysis** Phase. The various steps completed during this phase can be seen in **figure B.3.10**. The phase in question also should typically be performed for every cycle. An option whether this phase needs to be completed, as the case was for Project Planning, is given in cycles 2, 3 and 4 by means of a

message box. Therefore, if the current cycle is 2, 3 or 4, you can choose whether or not to perform the **Business Impact Analysis**.

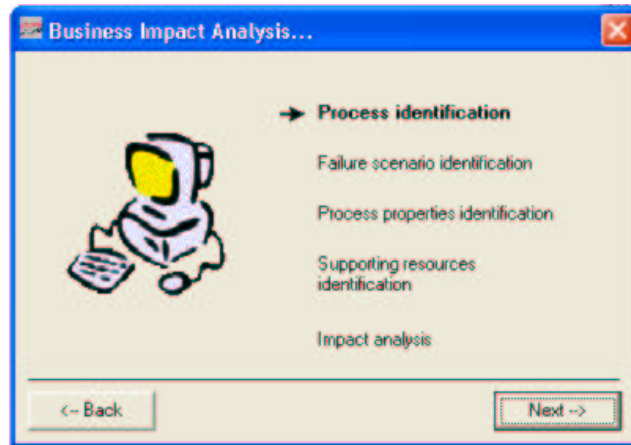


Figure B.3.10: The Business Impact Analysis wizard

- **Process identification**

The process identification procedure requires the listing of all the current business processes along with a short description of each. If the *Process identification* item is highlighted when the **Next ->** button is clicked, the process list screen, as shown in **figure B.3.11**, will be displayed. Here new processes can be added by clicking the **Add...** button or existing processes can be edited or deleted by means of the **Edit...** and **Delete...** buttons respectively. It should, however, be made clear that the deletion of a process will filter through all levels of plan information for the current plan. This means that if an existing process for which information has already been collected (possibly in preceding cycles) is deleted, all other related information (Supporting resources, Impact information etc.) will be lost as well.

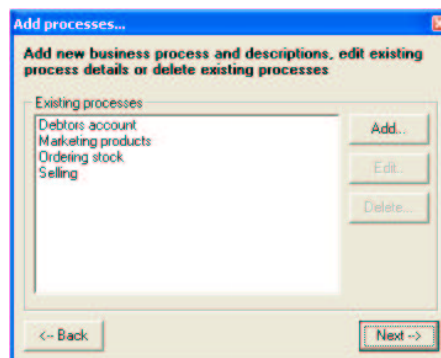


Figure B.3.11: The business process manipulation screen

In the screen, as shown above, clicking the **Add...** button will result in the display of the business process data capture screen, as shown in **figure B.3.12**.

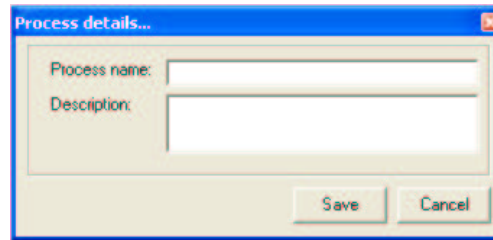


Figure B.3.12: The business process data capture

This screen requires only the process name and a short description of what function is performed by this process to be entered. To edit an existing process, simply select one of the items in the list as displayed in **figure B.3.11**, and click the **Edit...** button. This action will display a screen identical to the one in **figure B.3.12**, but populated with the information for the selected existing process. The deletion of a process will require you to confirm this action by means of a yes or no answer.

- **Failure scenario identification**

When the failure scenario identification item is highlighted, clicking the **Next ->** button will result in the display of a multi purpose list screen as shown in **figure B.3.7**. This screen will list all processes for the current plan. By clicking the **Add/Edit...** button you can identify a variety of failure scenarios for each process. If a certain process is selected from the list, clicking the **Add/Edit...** button will result in the display of the scenario data capture screen (**figure B.3.13**).

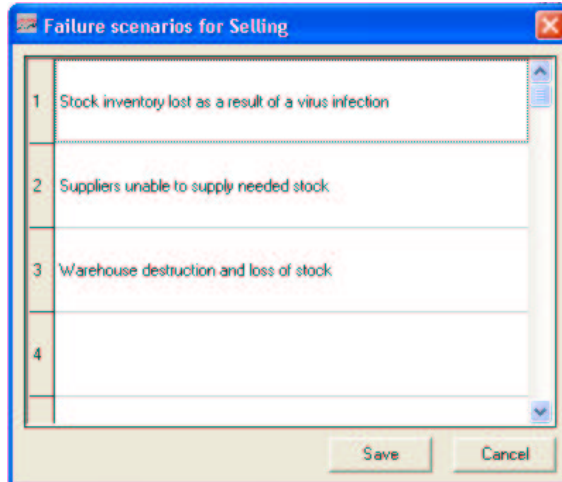


Figure B.3.13: The failure scenario data capture

To enter a scenario, simply click on one of the open slots (in the figure slot 4 is open) and enter the scenario. To proceed with the next scenario, click on another open slot when finished or press enter. Click on save when done to make sure all added scenarios are stored. If cancel is clicked all newly added scenarios will be lost.

- **Process properties identification**

When the process properties identification item is highlighted, clicking the button will also result in the display of the multi purpose list screen mentioned above. The process properties data capture screen will furthermore be displayed if a process is selected and the button is clicked. This screen is shown in **figure B.3.14**.

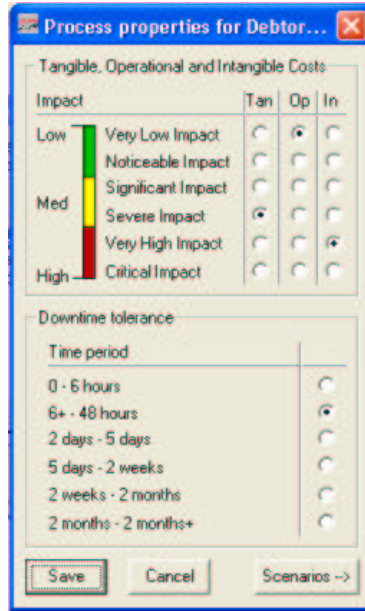


Figure B.3.14: The process properties data capture screen

For this procedure, simply click on the appropriate impact values for each process. Once this has been done for the four types of impacts, click the **Save** button to store these values. To view the failure scenarios for the current process, click on the **Scenarios -->** button to expand the current screen and show the process scenarios.

- **Supporting resources identification**

When the process supporting resources item is highlighted, clicking the **Next -->** button will also result in the display of a business process list screen. To add or edit supporting resources for a process, select a process from the list and click the **Add/Edit...** Button.

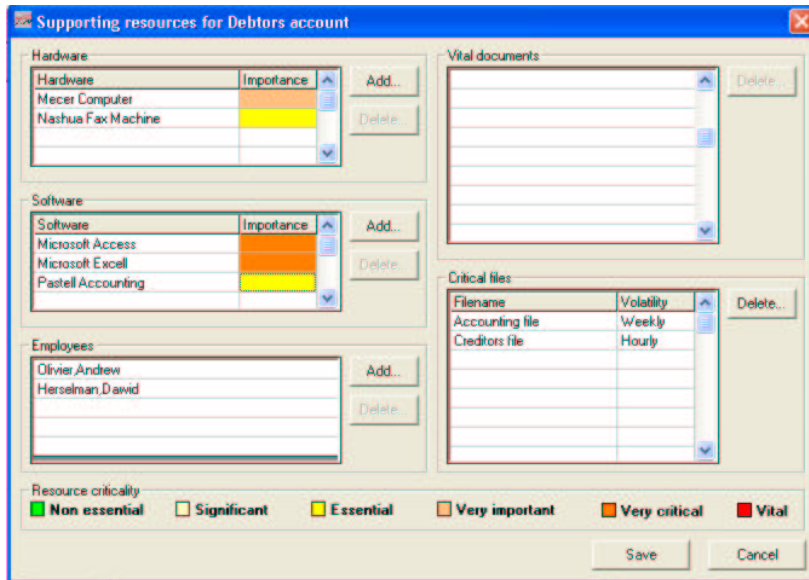


Figure B.3.15: The supporting resources data capture screen

To add hardware, software or employees for a specific process, click on the Add... button next to the appropriate grid. A screen containing a list of the required items will be shown. **Figure B.3.15** shows an example of such a list.

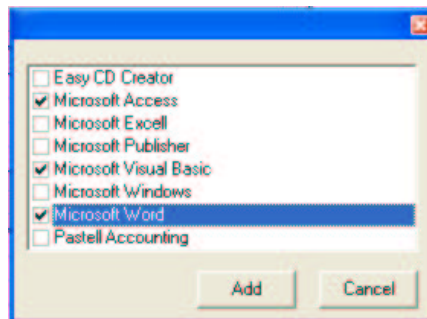


Figure B.3.16: A supporting resources list screen

Select the required items from this list. When done, click Add... and the items will be added to the appropriate grid. For hardware and software, the criticality of each resource should be indicated as well. When the resource is first added, the criticality is set to low by default. Clicking on the color in the grid will display alongside the original color. Select a color based on the legend at the bottom of the screen to indicate the appropriate criticality.

To add vital documents, simply click on an open slot to display a cursor and enter the document name. To enter more documents, select another open slot or press *Enter*.

To add critical file, also click on an empty slot, and enter the filename. How often each file changes or need to be backed up (i.e. the volatility) needs to be indicated as well. The default for each file is daily. Simply click on this value to change it. This will display a listing of available options alongside the original value. Simply click on the desired value to change it. When supporting resources identification is complete, click on to store the entered information.

- **Impact analysis**

If the impact analysis item is highlighted, clicking will display the impact analysis screen. This is simply an ordered list showing which business processes are the most critical and which processes could be regarded as non-essential.

3.2.1.3 Business Continuity Strategies

The third backup Cycle phase is the **Business Continuity Strategies** phase. Steps to be completed during this phase can be seen in **figure B.3.17**. For this cycle, only the first step will be completed. Note that the other Continuity Strategy steps are grayed out and will be completed in subsequent cycles.

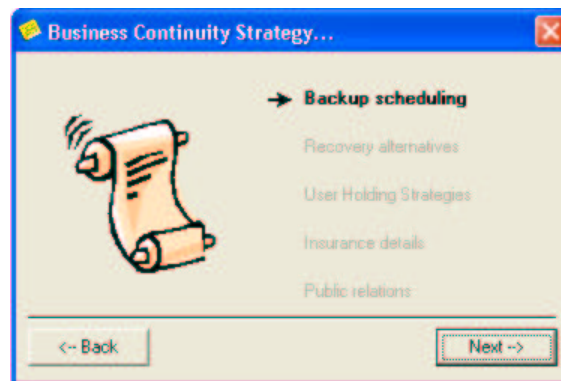


Figure B.3.17: The Business Continuity Strategies wizard

- **Backup scheduling**

When the backup scheduling step is highlighted, clicking the button will display a screen listing all business processes. To edit the backup schedules, simply

select the desired process from the list and click the **Add/Edit...** button. This will display the backup strategies screen, as seen in **figure B.3.18**.

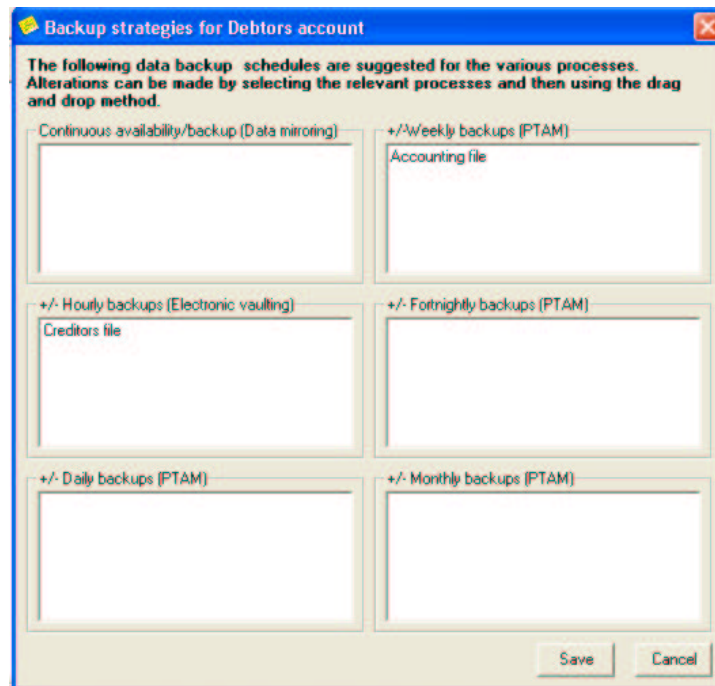


Figure B.3.18: A process backup scheduling screen

All files that have been identified during the **Business Impact Analysis** phase will be classified according to their volatility as identified earlier. If any of these files should be backup up more often or less often they could be dragged one at a time to the appropriate list by means of the drag and drop method.

3.2.1.4 Continuity Strategies Implementation

The Continuity Strategies Implementation phase is the fourth phase to be completed for the backup cycle. The various steps incorporated into this phase can be seen in **figure B.3.19**.

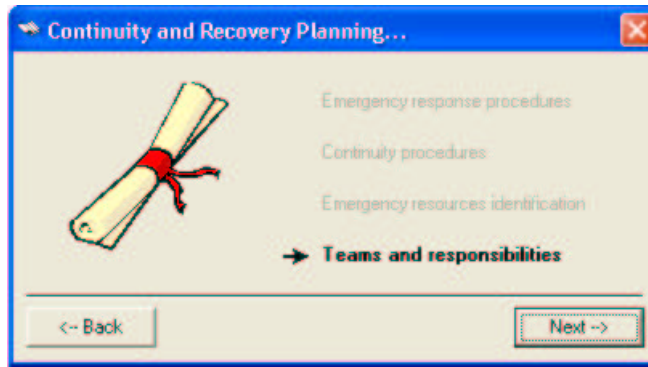


Figure B.3.19: The Continuity Strategies Implementation wizard

- **Teams and responsibilities**

The teams and responsibilities step is the only strategy implementation step to be completed during the backup cycle. It will, however, be completed for each of the subsequent cycles as well. The first screen in a set of 5 of screens for this step can be seen in **figure B.3.20**.

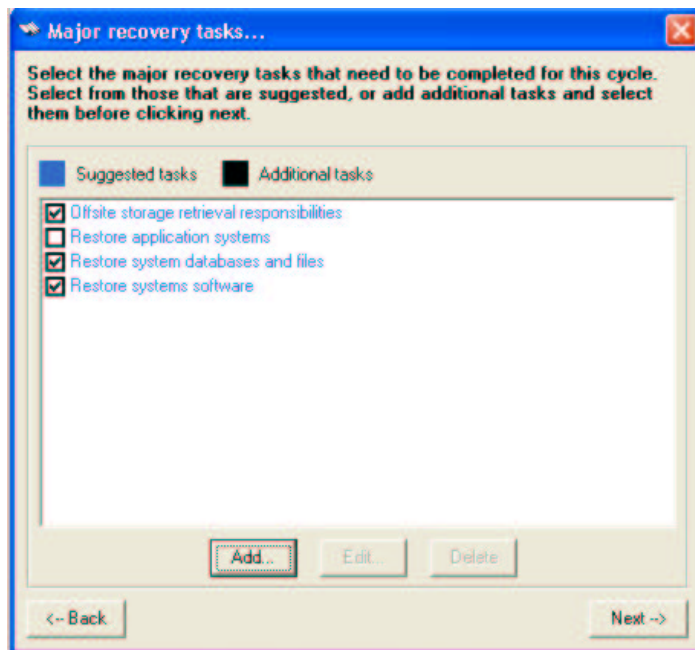


Figure B.3.20: The Major Recovery tasks screen

On this screen a list of suggested major recovery tasks is given. Choose from those that are given by checking each desired item. If additional tasks are required, they can be added by clicking the **Add...** button. If tasks need to be edited or deleted, select them one at a time by clicking on the list item (no checking required) and clicking the

or buttons. The highlighted item will then be edited or deleted. Please note that only additional tasks can be edited or deleted and not suggested tasks. Once this is done, click the button. The detailed recovery tasks screen will be displayed. This is shown in **figure B.3.21**.

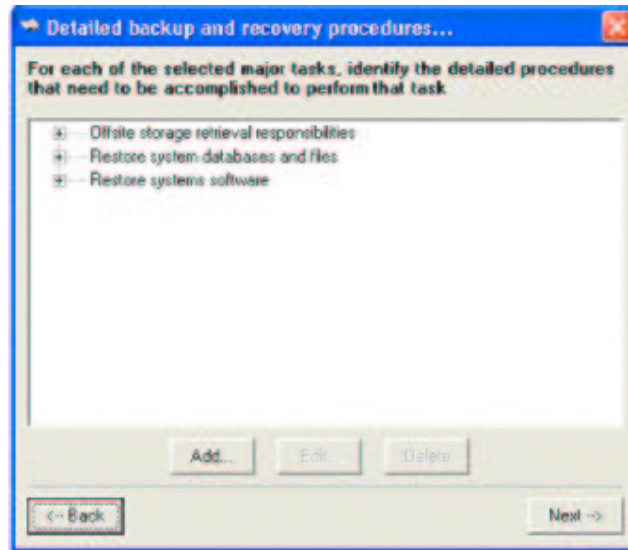


Figure B.3.21: The Detailed Recovery tasks screen

For each of the major recovery tasks chosen or added in the previous screen, detailed recovery tasks must now be added for each. To do this, select an item in the list displayed in **figure B.3.21** by clicking on it. Then click on the button. This will display the tasks capture screen. To add tasks, simply click anywhere on the grid where there is an open slot and then enter the task when the cursor appears. When data entry is completed, click the button. Those tasks that have been entered will have been added to the list on the detailed recovery tasks screen. To view these detailed tasks click on the sign. Only those major tasks that have detailed tasks added will display the sign.

The next step requires the definition of the required team(s) for this cycle. The next screen will display a list of existing teams. To add a team, click on the button and enter the team name and a brief team description. An example of this screen can be seen in **figure B.3.22**.

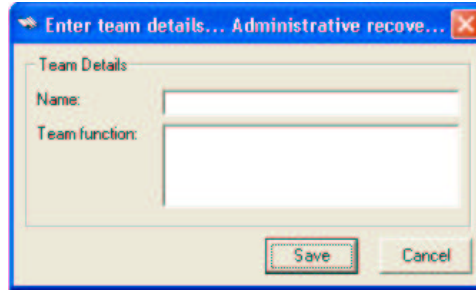


Figure B.3.22: Team details data capture screen

To edit or delete an existing team, simply select the team from the list and click on either the or button.

The next step involves identifying team members for the newly defined teams. This can be done by means of the screen depicted in **figure B.3.23**. To add a member to an existing team, select the team from the teams list and click the button located under the members list. This will display a list of all available employees. Select the employees to be assigned to the selected team and click . These members will then be added to the team.

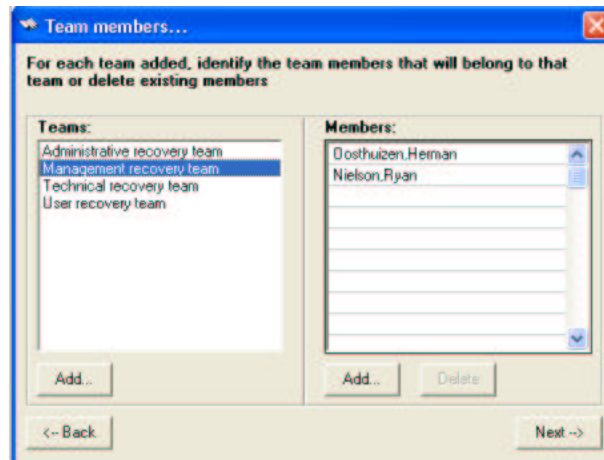


Figure B.3.23: Recovery team members screen

To delete an existing team member, select him/her from the members list and click . If an additional team is necessary, one can also perform this function by clicking the button. This will display the team details data capture screen as shown in **figure B.3.22**. A new team can then be added from here.

The last step in the *Teams and responsibilities* process is the assignment of the identified tasks to the appropriate team members. This can be done by means of the member responsibilities screen, shown in **figure B.3.24**.

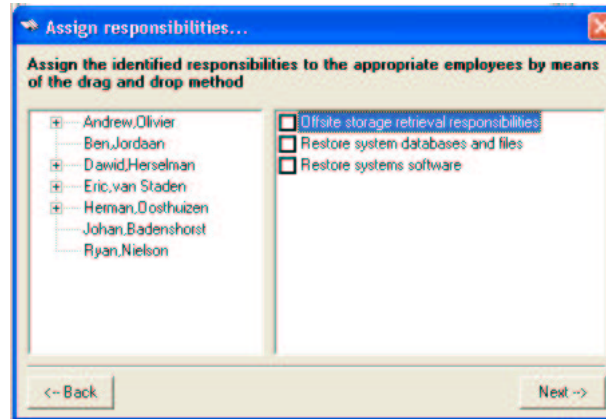



Figure B.3.24: Member responsibilities screen

To assign the responsibilities, select them from the list on the right hand side of the screen depicted in the above figure by checking a group of sub tasks or by checking the main task. This will automatically select all the sub-tasks as well. To assign these selected tasks, drag and drop them to the appropriate team member. This should be done until all the tasks have been assigned.

3.2.1.5 Testing

The next backup cycle task is **Test scheduling**. This can be done by means of the test schedule setup screen as shown in **figure B.3.25**. Tests can be of three types: Component, integrated and full tests. To add a specific test, click the  button for the required type of test.

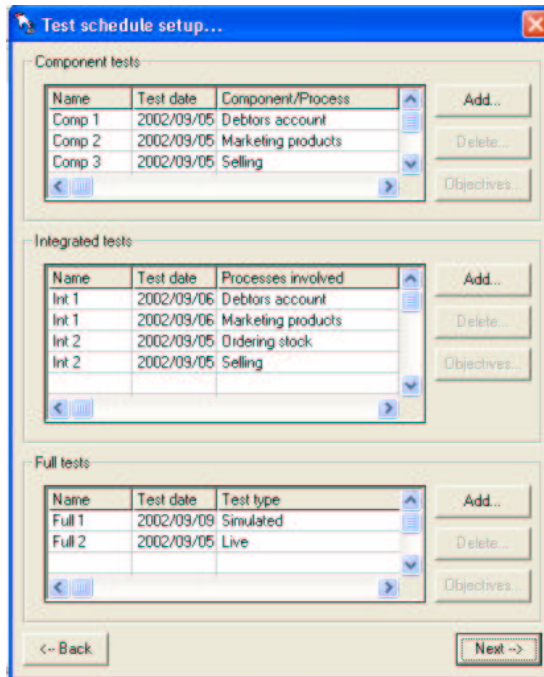


Figure B.3.25: Test schedule setup screen

The component test button allows for the scheduling of tests involving single business processes only. The screen with which to accomplish this is shown in **figure B.3.26**. Simply enter a test name, choose a date and select the process to be tested.

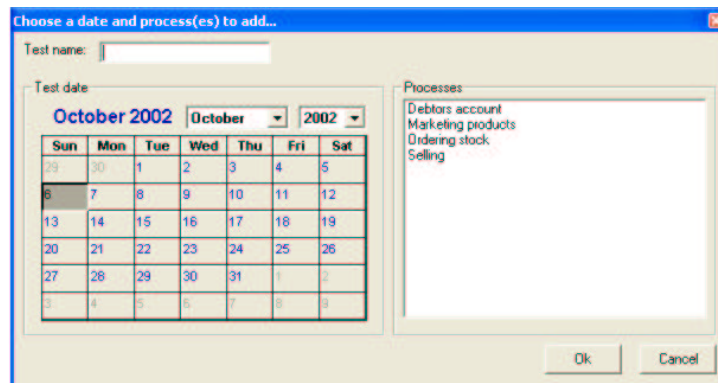






Figure B.3.26: Component test schedule screen

Scheduling integrated tests involves more or less the same procedure. The only difference is that the process list allows for the selection of more than one process. Therefore, for integrated tests, enter a test name, select a test date and select the appropriate business processes before clicking . Lastly, scheduling a full test would also require entering a test name, choosing a date and indicating whether this test is a live test or a simulation




before clicking . To delete a scheduled test, select the test by clicking on the test name within any one of the schedule grids. Then click on the  button to remove this test from the grid.

Test objectives could furthermore also be entered for each test by highlighting the appropriate test and clicking the  button. This will display a screen similar to that shown in **figure B.3.13**. To enter objectives for a specific test, select an open slot, click on it and enter the required objectives. Then click  to store the objectives.

3.2.1.6 Maintenance

The **Maintenance** phase is the final phase for this and all subsequent cycles. During this phase a maintenance committee and its members are identified either for this cycle or for all 4 cycles. All information is furthermore reviewed before the next cycle is started.

- **Establishing a committee**

Establishing a maintenance committee requires at least a team leader to be assigned. Therefore the adding of team members is optional. To add a team leader, click on the  button in line with the team leader data entry field. This will display an employee list of which only one list item can be chosen. To add team members, a similar procedure must be followed. Click on the  button to display an employee list. The difference between this list and the list mentioned above is that it can support multiple selections. Just select all the employees to be added and press .

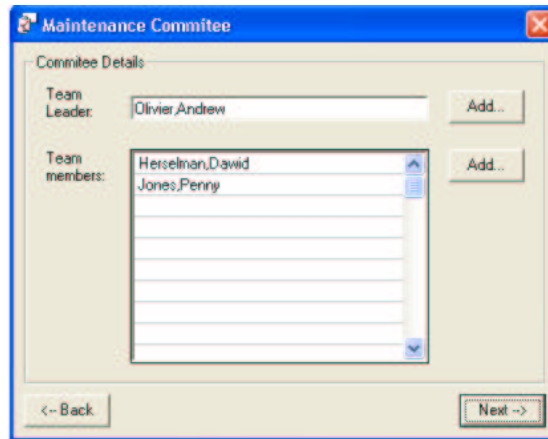


Figure B.3.27: Maintenance committee identification screen

- **Maintaining the plan**

The final step in the maintenance phase is the actual plan maintenance. **Figure B.3.28** shows a list of all information gathered during this cycle. To review a certain section of information, click on the item in the list to be reviewed. This will allow for that portion of information to be edited. Once this is completed, a ✓ will be placed along side the reviewed item to indicate completion. All items in the list should preferably be completely reviewed before proceeding with the next cycle.

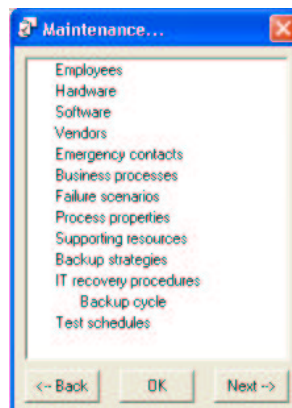


Figure B.3.28: Plan maintenance screen

3.2.2 The Disaster Recovery Cycle (Cycle 2)

For information on the **Project Planning, Business Impact Analysis, Testing and Maintenance** phases for this cycle, refer to section 3.2.1 for help.

3.2.2.1 Business Continuity Strategies

For the various steps to be completed during this phase refer to **figure B.3.17**. The **Business Continuity Strategies** for this cycle involves only the selection of processing alternatives.

- **Processing alternatives**

When is clicked the Alternate site identification screen is displayed. This screen can be seen in **figure B.3.29**. This screen will display a list of suggested processing alternatives. The selection is based on the criticality factors identified for each business process during the business impact analysis phase. Simply select one of the suggested alternatives and click to proceed.

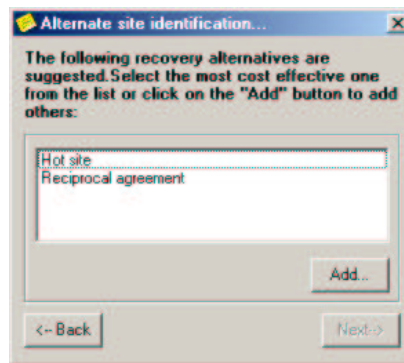


Figure B.3.29: Alternate site identification screen

The suggested alternatives list can be altered by clicking the button. This will display the available alternatives as seen in **figure B.3.30**. Select one or more alternatives from this list and click . These alternatives will then be added to the alternate site identification list in **figure B.3.29**.

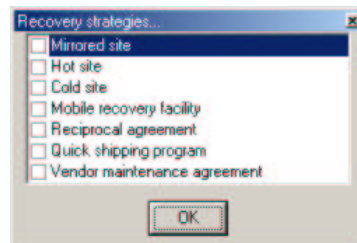




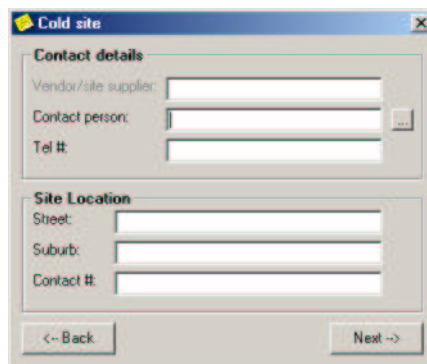


Figure B.3.30: Available alternatives listing

When  is clicked on the alternate site identification screen (**figure B.3.29**), the processing alternative details screen is displayed. This screen is shown in **figure B.3.31**. All alternate processing details must be entered except for the Vendor/supplier name, which is optional. This is because not all processing solutions involve vendors. For those that do not, the  button can be clicked to display a list of company employees. An employee can be selected and their name will be displayed in the *Contact person* field in **figure B.3.31**. This is the person responsible for all decisions regarding the alternate processing solutions.

If a vendor is, however, involved, the  button cannot be used. This is because the contact person then generally represents a vendor supplied contact person. When data entry is complete, the  button can be clicked to continue.



The screenshot shows a dialog box titled "Cold site" with a close button (X) in the top right corner. It is divided into two main sections: "Contact details" and "Site Location".

- Contact details:** This section contains three text input fields: "Vendor/site supplier:", "Contact person:", and "Tel #:". The "Contact person:" field has a small square button with three dots (...) to its right.
- Site Location:** This section contains three text input fields: "Street:", "Suburb:", and "Contact #:".


At the bottom of the dialog box, there are two buttons: "<-- Back" on the left and "Next -->" on the right.

Figure B.3.31: Processing alternatives' details

3.2.2.2 Continuity Strategy Implementation

For the various steps to be completed during this phase refer to **figure B.3.19**. The **Continuity Strategies Implementation** for this cycle involves the identification of emergency response procedures and team recovery responsibilities. For help on the recovery responsibilities, refer to section 3.2.1.2.

- o **Emergency response procedures**

Clicking  on the strategies implementation wizard screen will display the plan activations conditions screen. This screen is shown in **figure B.3.32**. BCP Cyclic makes use of three types of activation conditions as can be seen in the figure B.. These conditions assist in classifying a disaster when it strikes and to act appropriately.

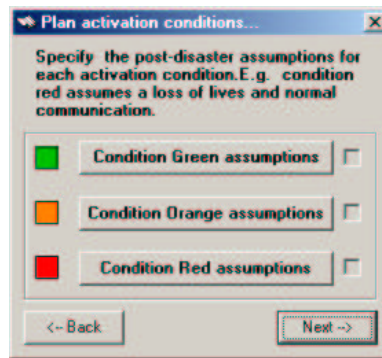


Figure B.3.32: Plan activation conditions screen

To add assumptions for a specific condition, click on that condition's assumptions button. This will display a screen allowing for the entry of one or more assumptions. Entries can be made on this screen by selecting an open slot and entering the identified assumptions. Those conditions for which assumption have already been entered will be indicated by . To continue, simply click . This will display the notification procedures screen shown in **figure B.3.33**.

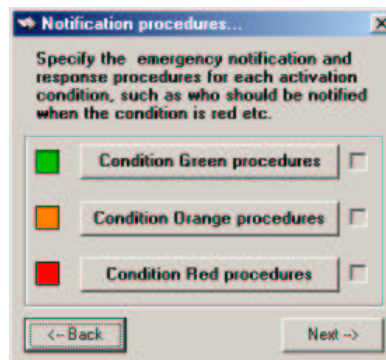


Figure B.3.33: Notification procedures screen

As for the plan activation conditions, the notification procedures must also be identified for each type of condition or at least for those that were chosen on the previous screen. The same procedures need to be followed to add notification procedures as was done for the activation conditions.

3.2.3 The Contingency Planning Cycle (Cycle 3)

For information on the **Project Planning**, **Business Impact Analysis**, **Testing** and **Maintenance** phases for this cycle, refer to section 3.2.1 for help.

3.2.3.1 Business Continuity Strategies

For the various steps to be completed during this phase refer to **figure B.3.17**. The **Business Continuity Strategies** for this cycle involves only the identification of appropriate user holding strategies for the various business processes.

- **User Holding Strategies**

Clicking on the business continuity strategies wizard screen will result in the display of a business process list screen as shown in **figure B.3.34**. To add holding strategies for a specific process or to edit them, select a process from the list and click button. This will display the holding strategies data capture screen as shown in **figure B.3.35**.

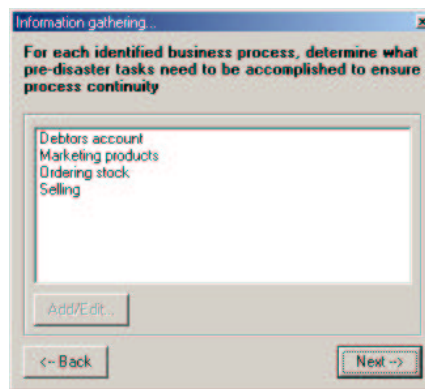


Figure B.3.34: Business process listing screen

To enter a holding strategy task, select an open slot, click on it and start typing as soon as the cursor appears. When all identified tasks for the specific process have been entered, click on the button. This will display the holding strategies responsibilities screen. This screen and its operations are similar to those of the member responsibilities screen as displayed in **figure B.3.24**. Simply drag and drop the tasks displayed in the list on the right to the appropriate employees listed on the left hand side.

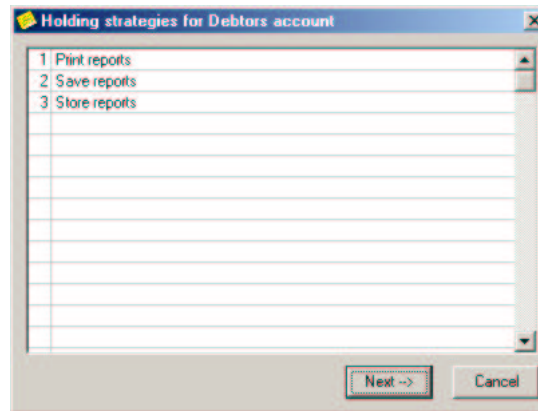


Figure B.3.35: Holding strategy data capture screen

3.2.3.2 Continuity Strategy Implementation

For the various steps to be completed during this phase refer to **figure B.3.19**. The **Continuity Strategies Implementation** for this cycle involves the identification of process continuity procedures and team recovery responsibilities. For help on the recovery responsibilities, refer to section 3.2.1.2.

- **Process continuity procedures**

Clicking on the strategies implementation wizard screen will display a business process list screen similar to that shown in **figure B.3.34**. To add or edit business continuity procedures for a specific process, select the process from the list and click the button. An employee list screen, as show in **figure B.3.37**, will be displayed.

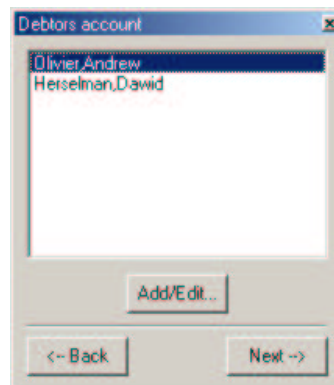




Figure B.3.37: Employee list screen

To enter each employee's continuity procedures, select an employee from the list displayed above and click . This will display a data capture screen similar to that shown in **figure B.3.35**. An employee's continuity procedures can be entered by selecting open slots on the above-mentioned screen and manually entering each employee's responsibilities when the cursor appears. When finished entering data, click  to store these responsibilities.

3.2.4 The Business Continuity Planning Cycle (Cycle 4)

For information on the **Project Planning, Business Impact Analysis, Testing and Maintenance** phases for this cycle, refer to section 3.2.1 for help.

3.2.4.1 Business Continuity Strategies

For the various steps to be completed during this phase refer to **figure B.3.17**. The **Business Continuity Strategies** for this cycle involves the recording of insurance details and public relation team details.

- **Insurance details**



When the  button is clicked when the Insurance details are highlighted, the Insurance details data capture screen, as shown in **figure B.3.38**, will be displayed. Simply enter all the details as requested by this screen along with the policy coverage details. These can be entered by selecting an open grid slot in the Policy coverage frame. When such a slot is clicked, a cursor will appear and the relevant information can be entered. To omit entering this information, simply click . If no information has been entered, or one or more field have been left out, you will be asked whether you want to continue nonetheless. Simply choose *Yes* to do so.

Figure B.3.38: Insurance policy details screen

- **Public relations details**

If the public relations item is highlighted, clicking the **Next ->** button will display the public relations responsibilities screen (shown in **figure B.3.39**). Information must be added for at least one employee. This would be the employee responsible for public relations within the organisation. To add one or more employees, click on the **Add...** button. A list of employees will be displayed. Select one or more employees by checking the checkboxes alongside each name and click **Ok**. All these names will then be added to the member field shown in **figure B.3.39**. For each added member, enter their responsibility by clicking on the Responsibilities field next to their names. A cursor will appear and text can be entered. When responsibilities have been entered for all members, click **Next ->**.



Member	Responsibilities/Roles

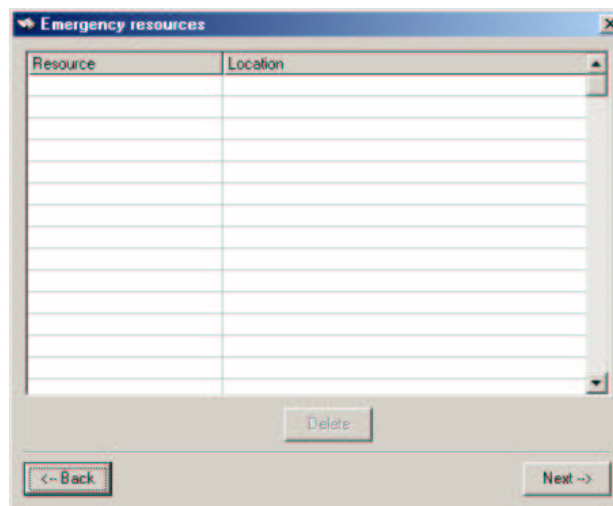
Figure B.3.39: Public relations details screen

3.2.4.2 Continuity Strategy Implementation

For the various steps to be completed during this phase refer to **figure B.3.19**. The **Continuity Strategies Implementation** for this cycle involves the identification of emergency resources and team recovery responsibilities. For help on the recovery responsibilities, refer to section 3.2.1.2.

- **Emergency resource identification**

When the emergency resources identification item is highlighted, clicking  will display the emergency resources data capture screen (shown in **figure B.3.40**). Resources can be added by selecting an open slot under the 'Resource' heading and entering a resource when the cursor appears. Once a resource has been entered, select an open slot under the 'Location' heading and do the same. When all resources and locations have been entered, click on  to continue.



Resource	Location

Figure B.3.40: Emergency resources data capture screen

3.3 The BCP Cyclic Menu and Toolbar Structure







The BCP Cyclic menu and toolbar are mainly utilised to manually add to or edit information contained within the application database. This database is used to store all created plans and associated details. Further menu and toolbar purposes will be discussed in the various sections below.



Figure B.3.41: The BCP Cyclic menu structure and toolbar

3.3.1 The File menu

BCP Cyclic file menu is shown in **figure B.3.42**. The various file menu commands will be discussed below and corresponding toolbar icons shown if applicable.

- **New**  : Starts the information gathering process for a new plan. The Information Gathering wizard (**figure B.3.3**) is shown.
- **Continue**  : Continue the information gathering process for an existing plan. The existing plan selection screen (**figure B.3.2**) is shown.
- **Open**  : Shows a file open dialogue box. This is used to select a saved business continuity plan or one of the available BCP Cyclic reports in text format and displays it.
- **Save**  : Shows a file save dialogue box. This is used to save the current business continuity plan or one of the produced BCP Cyclic reports in text format and to open at a later stage
- **Build plan**  : When one or more cycles have been completed, this is used to produce a plan containing the information gathered so far
- **Exit**  : Closes the BCP Cyclic application

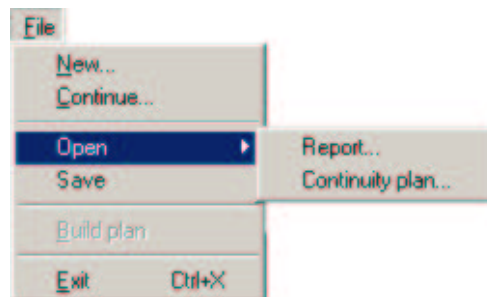


Figure B.3.42: The BCP Cyclic file menu

3.3.2 The View menu

The BCP Cyclic view menu is shown in **figure B.3.43**. Its function and commands will be discussed below.

- **Toolbar** : Shows or hides the BCP Cyclic toolbar. If a checkmark is shown the toolbar should be visible.
- **Statusbar** : Shows or hides the BCP Cyclic statusbar. If a checkmark is shown the statusbar should be visible.

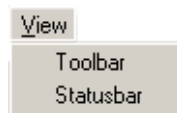



Figure B.3.43: The BCP Cyclic view menu

3.3.3 The Planning menu

To edit planning details, simply click on the Planning menu, or click on the  icon on the toolbar, This will display either a menu list as displayed in **figure B.3.44** or a toolbar menu displayed in **figure B.3.45**.

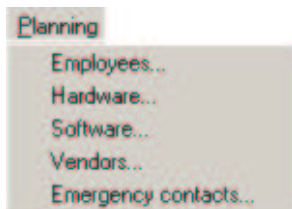


Figure B.3.44: Planning menu structure



Figure B.3.45: Planning toolbar menu

Select the menu item for which you want to add or edit details from the menus displayed above. Then follow the procedures as described in section 3.2.1.1.

3.3.4 The BIA menu


To edit planning details, simply click on the *Planning* menu, or click on the  icon on the toolbar, This will display either a menu list as displayed in **figure B.3.46** or a toolbar menu displayed in **figure B.3.47**.




Figure B.3.46: Planning menu structure



Figure B.3.47: Planning toolbar menu

Select the menu item for which you want to add or edit details from the menus displayed above. Then follow the procedures as described in section 3.2.1.2.

3.3.5 The Strategies menu

To edit planning details, simply click on the Planning menu, or click on the  icon on the toolbar. This will display either a menu list as displayed in **figure B.3.48** or a toolbar menu displayed in **figure B.3.49**.

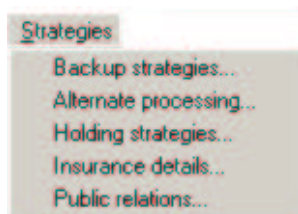


Figure B.3.48: Planning menu structure

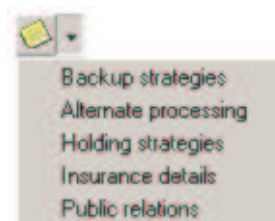



Figure B.3.49: Planning toolbar menu

Select the menu item for which you want to add or edit details from the menus displayed above. Then follow the procedures as described in sections 3.2.1.3, 3.2.2.1, 3.2.3.1 and 3.2.4.1.

3.3.6 The Implementation menu

To edit planning details, simply click on the *Planning* menu, or click on the  icon on the toolbar. This will display either a menu list as displayed in **figure B.3.50** or a toolbar menu displayed in **figure B.3.51**.

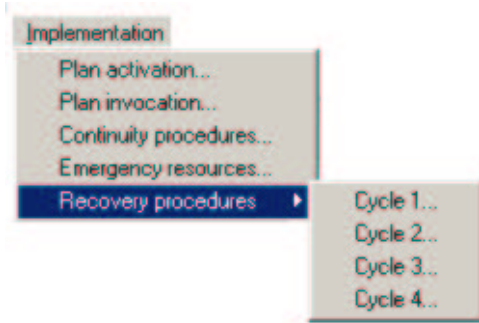



Figure B.3.50: Planning menu structure

Select the menu item for which you want to add or edit details from the menus displayed above. Then follow the procedures as described in sections 3.2.1.4, 3.2.2.2, 3.2.3.2 and 3.2.4.2.

3.3.7 The Testing menu

To edit planning details, simply click on the Planning menu, or click on the  icon on the toolbar. This will display menu list as displayed in **figure B.3.52**.

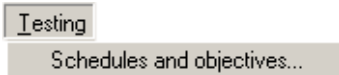



Figure B.3.52: Planning menu structure

Select the menu item for which you want to add or edit details from the menus displayed above. Then follow the procedures as described in section 3.2.1.5.

3.3.8 The Maintenance menu

To edit planning details, simply click on the *Planning* menu, or click on the  icon on the toolbar. This will display either a menu list as displayed in **figure B.3.53** or a toolbar menu displayed in **figure B.3.54**.

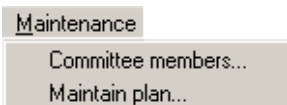


Figure B.3.53: Planning menu structure

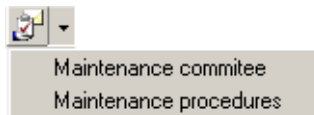


Figure B.3.54: Planning toolbar menu

Select the menu item for which you want to add or edit details from the menus displayed above. Then follow the procedures as described in section 3.2.1.6.

3.3.9 The Reports menu

The reports menu, shown in **figure B.3.55**, is used to produce sections of the business continuity plan on command. The figure shows a list of available reports. Simply select a report from the list. The BCP Cyclic database will be accessed and the report will be displayed.

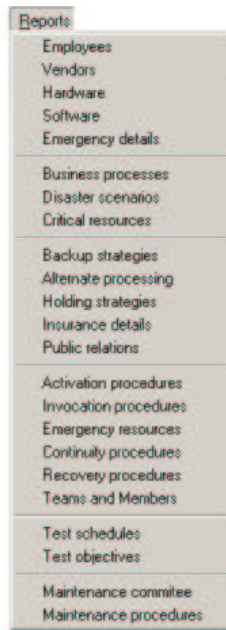


Figure B.3.55: Reports toolbar menu

ANNEXURE C

BCP Cyclic

Prototype Output

Output Related Aspects

Please note the following with respect to the output produced by the BCP Cyclic prototype:

- All information gathered during the case study has been included in this annexure. The output has, however, been altered slightly to ensure that it is in a presentable format as well as to protect the identity of the organisation.
 - The output displayed in this annexure is not in any specific format, but simply a printout of information obtained during the case study. The BCP Cyclic package is still in prototype form and will produce output in a more presentable format once completed.
 - Some of the information in this annexure has been altered because of shortcomings in the prototype. An example of this is the backup strategies that had to be updated due to information gathering compatibility issues within the prototype.
-

1. Introduction

1.1 Policy statement

It shall be the policy of **Organisation A** to provide a survival plan to protect the assets, accurate records, the well-being and safety of employees and to provide for the continuation of essential services to the organisation and to its customers.

The plan will provide for the re-establishment of operations within _____ hours of a declared disaster.

The plan will provide for the restoration of these critical operations in the defined priority sequence.

The plan will be the responsibility of **Employee 5** to ensure continued maintenance and quarterly reviewing and testing.

Approved by: _____
Title: _____

1.2 Plan scope

Place the scope of the plan here.

(The scope should specify what business activities the plan will address. The plans boundaries and exclusions should be included. The boundaries will place limits of what the plan will cover and the exclusions are those issues that will not be addressed by the plan.)

1.3 Plan objectives

The objectives of the survival plan are to provide a programme to achieve the following ends of the event of a disaster in the facilities of **Organisation A** located in **Port Elizabeth**.

Major objectives:

To continue operations in order to maintain essential customer services, to continue support services to maintain cash flow and to maintain the confidence of customers, vendors, employees and shareholders.

To provide for the restoration of critical operations within ___ hours.

To provide for the restoration of all operations within ___ days.

To achieve the foregoing in a cost effective manner.

1.4 Plan assumptions

Type plan assumptions here.

2. Business Impact Analysis

2.1 Critical processes

Name: Freight process
Description: Communication with freight companies to arrange product deliveries
State: Very critical
Recovery time: 0-6 hours
Tangible costs: 6
Intangible costs: 5
Operational costs: 3

Name: Communication
Description: Communicating with various organisational franchises
State: Very critical
Recovery time: 6-48 hours
Tangible costs: 4
Intangible costs: 5
Operational costs: 2

Name: Process orders
Description: Managing orders placed via e-mail or fax
State: Vital
Recovery time: 2-5 days
Tangible costs: 3
Intangible costs: 5
Operational costs: 3

Name: Payroll
Description: Processing employee salaries, PAYE, Tax, requests for leave etc.

State: Very important
Recovery time: 2-5 days
Tangible costs: 1
Intangible costs: 1
Operational costs: 1

Name: Accounting
Description: Managing the financial aspect of the organisation
State: Very important
Recovery time: 2-5 days
Tangible costs: 5
Intangible costs: 2
Operational costs: 2

2.2 Supporting resources

Process name: Accounting

Hardware:

- PC 2
- File Server
- HP Deskjet 845
- PC 5
- Lexmark Laser Printer

Software:

- Microsoft Office 2000 Professional
- Pastell Partner

Employees involved:

- Employee 2
 - Employee 5
-

Process name: Communication

Hardware:

- PC 1
- PC 3
- HP Deskjet 610C (1)
- HP Deskjet 610C (2)
- HP Deskjet 845
- PC 5

Software:

- Microsoft Internet Explorer
- Microsoft Office 2000 Professional

Employees involved:

- Employee 1
 - Employee 2
 - Employee 3
 - Employee 4
 - Employee 5
 - Employee 6
 - Employee 7
-

Process name: Freight process**Hardware:**

- PC 3
- HP Deskjet 610C (1)

Employees involved:

- Employee 5
 - Employee 7
-

Process name: Payroll**Hardware:**

- PC 2
- Dot Matrix
- Epson
- PC 5
- Lexmark Laser Printer

Software:

- VIP GT Payroll

Employees involved:

- Employee 2
- Employee 5

Miscellaneous documents:

- Clockcards

Process name: Process orders**Hardware:**

- PC 2

- File Server
- HP Deskjet 610C (1)
- PC 5
- Lexmark Laser Printer

Software:

- Microsoft Office 2000 Professional
- Pastell Partner

Employees involved:

- Employee 1
- Employee 2
- Employee 4
- Employee 5
- Employee 7

3. Business Continuity Strategies

3.1 Backup strategies

Organisation A makes use of centralised server backups. Data is backed up daily by means of the backup utility provided by Windows NT server and backed up by means of a tape backup system. Data backup occurs automatically at 19h00 each day. Backups are performed as follows:

- A full backup of all data stored on the file server
- Incremental backups performed daily thereafter of all files that have changed

Organisation A makes a copy of each backup. One copy is stored on site and the other transported to the alternate processing facility. **Employee 5** is responsible for the entire backup process.

3.2 Alternate processing locations

Organisation A have selected a Mirrored site as a solution for IT recovery.

Include a brief description of the alternate location and it's facilities here.

Site details are as follows:

Vendor: N/A
Contact: Employee 5
Telephone: (041)1234567
Street: 100 2nd Avenue
Suburb: Walmer
Site: (041)7654321

3.3 User holding strategies

Process name: Accounting

Employee 2:

- Regularly print and store list of creditors
- Regularly print and store list of Pastell accounts
- Store bank statements
- Store supplier invoices

Process name: Payroll

Employee 2:

- Store clockcards
- Store payslips

Process name: Process orders

Employee 5:

- Store invoices(pro-forma & commercial)
- Store order confirmation sheets
- Store order forms

3.4 Insurance details

Company: Insurance company 1
Contact: Employee 1
Telephone: (041)1234567
Street: 150 3rd avenue
Suburb: Newton Park
Code: 1234
City: Port Elizabeth

Policy coverage: Fire
Floods
Payroll
Loss of income

3.5 Public relations

The following individuals have been made responsible for any public relations related tasks:

- Employee 1 Company director
- Employee 3 Company director
- Employee 5 Company director

4. Continuity Strategies Implementation

4.1 Emergency response procedures

Condition Red Assumptions:

- Notify all relevant personnel
- Notify relevant emergency services
- Relocate personnel to offsite location

4.2 Plan invocation procedures

Condition Red Procedures:

- Individual PC failure
- Peripheral device failure
- Loss of communications network (including telephone)
- Loss of entire IT infrastructure
- Loss of office facilities

4.3 Process continuity procedures

Process name: Accounting

Employee 2:

- Handle reconciliation
- Print weekly bank statements
- Sort mail
- Write orders & attach invoices

Employee 5:

- Check allocation of financial transactions
- Property trust books responsibilities

Process name: Communication

Employee 1:

- Answer all technical queries via e-mail

Employee 3:

- Handle all franchise related queries
- Responsible for developing new franchises
- Responsible for sales & marketing

Process name: Freight process

Employee 7:

- Coordinate freight deliveries
- Freight forwarding

- Preparing freight documentation

Process name: Payroll

Employee 2:

- Loan processing
- Print payslips
- Process weekly wages
- Update leave records

Employee 5:

- Administrate leave
 - Check payslips
 - Install new versions of payroll software
-

Process name: Process orders

Employee 1:

- Ensure adequate product availability

Employee 4:

- Ensure correct package labelling
- Ensure orders are packaged correctly

Employee 7:

- Confirm orders
- Generate and prepare order sheets
- Prepare and process pro-forma invoices

4.4 IT recovery procedures

Backup cycle procedures

Employee 5:

- Install Mercury Mail
- Install Windows NT Server
- Install Winproxy
- Restore backups from tapes
- Test service provider connection
- Connect PCs to server
- Install relevant operating system
- Load relevant applications
- Set up printers

Recovery cycle procedures

Employee 5:

- Assess disaster severity
- Contact relevant emergency services
- Restore/ensure web site integrity
- Restore intranet

4.5 Team details

Team: **Technical recovery team**

Description: Restore data and software, maintain IT infrastructure

Member(s): Employee 5

5. Plan Maintenance

5.1 Maintenance committee

Team leader: Employee 5

6. Appendix A

6.1 Employees

Name: Employee 1
Department: N/A
Job Title: N/A
Address: 1 1st avenue
Walmer
Port Elizabeth
6070
Tel(H): (041) 555 1234
Tel(W): (041) 506 1111
Cellphone: 0831234567

Name: Employee 2
Department: N/A
Job Title: N/A
Address: 2 2nd avenue
Walmer
Port Elizabeth
6070
Tel(H): (041) 555 5678
Tel(W): (041) 506 2222
Cellphone: 0837654321

Name: Employee 3
Department: N/A
Job Title: N/A
Address: 3 3rd avenue
Walmer
Port Elizabeth
6070
Tel(H): (041) 555 4321
Tel(W): (041) 506 3333
Cellphone: 0836543217

Name: Employee 4
Department: N/A
Job Title: N/A
Address: 4 4th avenue
Walmer
Port Elizabeth
6070
Tel(H): (041) 555 8765
Tel(W): (041) 506 4444
Cellphone: 0835432167

Name: Employee 5
Department: N/A
Job Title: N/A
Address: 5 5th avenue
Walmer

Port Elizabeth
6070
Tel(H): (041) 555 7654
Tel(W): (041) 506 5555
Cellphone: 0834321567

Name: Employee 6
Department: N/A
Job Title: N/A
Address: 6 6th avenue
Walmer
Port Elizabeth
6070
Tel(H): (041) 555 6543
Tel(W): (041) 506 6666
Cellphone: 0833214567

Name: Employee 7
Department: N/A
Job Title: N/A
Address: 7 7th avenue
Walmer
Port Elizabeth
6070
Tel(H): (041) 555 5432
Tel(W): (041) 506 7777
Cellphone: 0832134567

6.2 Hardware

Name: PC 1
Type: PC
Description: Celeron 500 Mhz, 96 MB RAM,4.3 MB Hard Disk
Vendor: Vendor A
Department: N/A

Name: PC 2
Type: PC
Description: P II 333Mhz, 128 MB RAM,4.3 GB Hard Disk
Vendor: Vendor D
Department: N/A

Name: PC 3
Type: PC
Description: Celeron 400 Mhz,64 MB RAM,4.3 GB Hard Disk
Vendor: Vendor A
Department: N/A

Name: Dot Matrix
Type: Printer
Description: None
Vendor: Vendor C
Department: N/A

Name: Epson
Type: Printer
Description: None
Vendor: Vendor D
Department: N/A

Name: File Server
Type: None
Description: P III 1 Ghz, 128 MB RAM, 20 GB Hard Disk
Vendor: Vendor A
Department: N/A

Name: PC 4
Type: PC
Description: Pentium 75 Mhz,32 MB RAM,4.3 GB Hard Disk
Vendor: Vendor B
Department: N/A

Name: HP Deskjet 610C (1)
Type: Printer
Description: None
Vendor: Vendor B
Department: N/A

Name: HP Deskjet 610C (2)
Type: Printer
Description: None
Vendor: Vendor C
Department: N/A

Name: HP Deskjet 845
Type: Printer
Description: None
Vendor: Vendor A
Department: N/A

Name: PC 4
Type: PC
Description: P III 800 Mhz, 128 MB Ram, 10 GB Hard Disk
Vendor: Vendor B
Department: N/A

Name: Lexmark Laser Printer
Type: Printer
Description: None
Vendor: Vendor D

Department: N/A

Name: PC 5
Type: PC
Description: 233 Mhz,64 MB RAM,4.3 GB Hard Disk
Vendor: Vendor A
Department: N/A

Name: Notebook
Type: Notebook
Description: Pentium,32 MB RAM,2.1 GB Hard Disk
Vendor: Vendor C
Department: N/A

Name: Scanning PC
Type: PC
Description: Celeron 400 Mhz, 64 MB RAM, 4.3 GB Hard Disk
Vendor: Vendor D
Department: N/A

Name: PC 6
Type: PC
Description: Celeron 400 Mhz,64 MB RAM, 4.3 GB Hard Disk
Vendor: Vendor A
Department: N/A

6.3 Software

Name: Adobe Acrobat Reader
Version: 4
Type: None
Vendor: Vendor D
Department: N/A

Name: Arcsoft
Version: Unknown
Type: None
Vendor: Vendor G
Department: N/A
Name: CashPlan
Version: Unknown
Type: None
Vendor: Vendor G
Department: N/A

Name: Dazzle DPM
Version: Unknown
Type: None
Vendor: Vendor F
Department: N/A

Name: Hewlett Packard Scanning
Version: Unknown
Type: Scanning software
Vendor: Vendor A
Department: N/A

Name: Lotus Smartsuite
Version: Unknown
Type: None
Vendor: Vendor H
Department: N/A

Name: Mercury Mail
Version: Unknown
Type: E-mail
Vendor: Vendor H
Department: N/A

Name: Microsoft Internet Explorer
Version: Unknown
Type: Internet Browser
Vendor: Vendor H
Department: N/A

Name: Microsoft Office 2000 Professional
Version: Unknown
Type: None
Vendor: Vendor A
Department: N/A

Name: Microsoft Office 2000 Standard
Version: Unknown
Type: None
Vendor: Vendor D
Department: N/A

Name: MS Encarta Encyclopedia 2000
Version: Unknown
Type: None
Vendor: Vendor G
Department: N/A

Name: MS Excel 97
Version: Unknown
Type: Spreadsheet
Vendor: Vendor G
Department: N/A

Name: MS Publisher 98
Version: Unknown
Type: Publishing software
Vendor: Vendor A
Department: N/A

Name: NAV2000
Version: Unknown
Type: None
Vendor: Vendor D
Department: N/A

Name: Nero Burning
Version: Unknown
Type: CDR/W Burning software
Vendor: Vendor F
Department: N/A

Name: Nikon Views
Version: Unknown
Type: None
Vendor: Vendor F
Department: N/A

Name: Pastell Partner
Version: 5.2
Type: None
Vendor: Vendor D
Department: N/A

Name: Power Director Pro
Version: Unknown
Type: None
Vendor: Vendor G
Department: N/A

Name: Standard Bank
Version: Unknown
Type: None
Vendor: Vendor G
Department: N/A

Name: VIP GT Payroll
Version: Unknown
Type: None
Vendor: Vendor H
Department: N/A

Name: Windows 95
Version: Unknown
Type: Operating System
Vendor: Vendor F

Department: N/A

Name: Windows 98
Version: Unknown
Type: Operating System
Vendor: Vendor A
Department: N/A

Name: Windows NT Server
Version: Unknown
Type: Operating System
Vendor: Vendor D
Department: N/A

Name: Windows NT Service Pack
Version: 6
Type: None
Vendor: Vendor D
Department: N/A

Name: Winproxy
Version: 4
Type: None
Vendor: Vendor G
Department: N/A

Name: Winzip
Version: Unknown
Type: Compression software
Vendor: Vendor A
Department: N/A

ANNEXURE D

Paper submitted to Information Management
& Computer Security

‘A Cyclic Approach to Business Continuity
Planning’

A CYCLIC APPROACH TO BUSINESS CONTINUITY PLANNING

Jacques Botha and Rossouw Von Solms
Department of Information Technology
Port Elizabeth Technikon
Port Elizabeth

Abstract

In a world where continuous operations are essential for business survival, action must be taken to ensure information and the business processes that use the information are continuously available. This usually involves the selection and implementation of a suitable business continuity plan. Implementing such a plan is, however, not always a simple task. This especially holds true for small to medium sized organizations. An implementation method that could be applied to most Business Continuity Planning (BCP) methodologies would, therefore, be a welcome tool, especially for small to medium sized organisations.

1. Introduction

The Information Technology (IT) industry has advanced rapidly over the years, so much so that it now forms a vital component for conducting business (von Solms, 1999). The majority of organisations cannot do without their computer systems in this day and age. As these systems evolve, they also need to be protected against today's considerable amount of threats to the information they process, transmit and store (Halliday, Badendorst & von Solms, 1996). An IT failure or disaster could, therefore, have serious consequences for an organisation (IBM Global Services, 2000).

When the word disaster is mentioned, events like earthquakes, fires and floods come to mind. However, system malfunctions and computer viruses can be regarded as disasters as well and are after all more common occurrences (Hawkins, Yen & Chou, 2000). Business Continuity Planning (BCP) involves developing a collection of procedures for the various business units that will ensure the continuance of critical business processes while the data centre is recovering from the disaster (Wilson, 2000).

For organisations that fall into the category of small or medium, the development of a business continuity plan could prove difficult. Literature aimed at the development of a business continuity plan seldom concentrates on smaller organisations (Weems, 1999). Furthermore, through the study of various methodologies it is clear that the majority of literature seldom describes how these methodologies should be implemented.

The rest of this paper will not only motivate and discuss a complete seven phase BCP methodology, but will also discuss an implementation method for this BCP methodology. The aforementioned implementation method will simplify the BCP process for organisations and should be applicable to most continuity planning methodologies.

2. Information Security and Business Continuity Planning

Information possessed by organisations is no longer only used by employees, but by customers and partners as well. These users expect continuous availability of and instantaneous access to organisational information (McAnally, DiMartini, Hakun, Lindman & Parker, 2000). Protecting their information is essential to ensure that the business has a competitive edge and maintains cash flow and commercial image (BS7799-1, 1999, p.1). In order to ensure that an organisation maintains its competitive edge, the information must be kept confidential, accurate and continuously available.

Although ensuring confidentiality and integrity is important, the availability component of information security is of greater importance with respect to BCP. Organisations nowadays are competing on a global scale and require high availability levels of information technology resources and services (Glorioso & Desautels, 1999). To completely define BCP one has to consider two aspects. Firstly, it should be ensured that an organisation could continue business as usual, or on an acceptable level in the wake of disaster. Secondly, IT should be restored to a state similar to that preceding the disaster (Glenn, 2002). To better understand these two components of BCP, the concepts Contingency Planning and Disaster Recovery Planning (DRP) have to be considered.

The aim of Contingency Planning is to make provision for continuing business processes in a disaster situation while recovery is taking place (Glenn, 2002). It can be defined as the process of examining an organisation's critical functions, identifying the possible disaster scenarios and developing procedures to address these concerns (Rubin, 1999, p. 73). DRP was originally intended for operations established to minimise data centre downtime. Today DRP is seen as the active component of BCP and focuses mainly on the recovery of the IT department and all related functions (Hassim, 2000).

Keeping the above definitions in mind, BCP can be defined as a complete process of developing measures and procedures to ensure an organisation's disaster preparedness. This includes ensuring that the organisation would be able to respond effectively and efficiently to a disaster and that their critical business processes can continue as usual. (Business Contingency Preparedness, 2002). Although authors differ on the precise and clear distinction between the three processes, the inter-relationship of these processes, as defined in this paper, is depicted in figure 1. The smaller circles labelled A to I represent various business processes. These processes are all dependant on services and infrastructure provided by the IT Department, depicted by the innermost circle in the figure. Some of these processes are also dependant on others, as depicted by adjacent circles. The outermost circle represents a combination of the disaster recovery plan for the IT department and the contingency plans for these various business processes.



Figure 1: BCP, CP and DRP relationship

3. Business Continuity Planning in Smaller Organisations

The majority of the information relating to BCP usually discusses the development of continuity plans for large organisations, omitting how this process might differ in smaller organisations. Resources and staff are unfortunately limited, especially when it comes to smaller companies. The BCP project is also a non-revenue producing project and does not qualify as a high priority project for organisations (Weems, 1999).

There are various different sources that categorize Small to Medium Enterprises (SMEs). The categorisation is largely dependant on factors such as the country where the organisation is located and the type of organisation or business (Bowler & Dawood, 1995). There are generally two main distinguishing factors for small and large organisations. These are workforce size, and annual revenue and turnover (Meggison, 1994). There are, however, other factors that further distinguish small and large companies. These are discussed below along with their possible effect on BCP.

- **Financial performance:** SMEs, on average and proportional to size, perform better financially than large organisations (Griffin, 1990).
- **Innovation:** Small organisations promote individual resourcefulness due to a less restrictive environment (Barrow, 1993). SME employees' area of expertise is furthermore wide ranging (Johnson, 2002)
- **Job Creation:** The rate of job creation in smaller organisations is much higher than in larger organisations (Griffin, 1990). SMEs across all sectors show rapid growth compared to larger businesses, especially with respect to workforce size (Barrow, 1993).
- **Contributions to larger organisations:** Most of the suppliers to large businesses are smaller organisations. SMEs are key players in product distribution and selling for larger organisations (Griffin, 1990).
- **SME environments:** SMEs are very much dependent on the state of the market. Changes in economic conditions force them to change as well (Barrow, 1993). Smaller organisations can, therefore, be seen as operating in more dynamic environments than larger firms.
- **Management structure:** Smaller organisations have a flatter management structure than their larger counterparts. (Devargas, 1999, p. 35). In small organisations managers are usually directly involved in the day-to-day activities and are also closer to their employees (Johnson, 2002).
- **Infrastructure complexity:** In general, the size of an organisation directly impacts the costs for these organisations, especially when recovery strategies are involved. Hardware and software for smaller organisations tend to be less costly than for large organisations. (Beckmeyer, 2001).
- **SME budgetary issues:** The tendency for organisations is to set aside approximately two percent of IT budgets for BCP (Jackson & Carey, 1997).

Unfortunately SMEs do not have a large budget in general (Weems, 1999). It could further be assumed that the IT budget, and the BCP budget, will be limited for SMEs.

- **SME conduct:** Small organisations are generally less formal in the way operations are conducted. This usually leads to a more casual control environment (Johnson, 2002).

From the above described characteristics two important issues have come to light. This is, firstly, that there might be a difference in some aspects of the BCP process for smaller organisations. Secondly, that some organisations might want to implement a BCP methodology in a different manner. Small and large organisations do, however, generally have to address the same BCP issues (Weems, 1999). Therefore, instead of having two different methodologies for small and large organisations, it would make more sense to create a methodology that is scalable to cater for all organisations. An implementation approach that allows for the implementation of only certain BCP aspects that depend on organisational requirements could also be useful. The next two sections will discuss suggested solutions to the above-mentioned problems.

4. A Seven-Phased Business Continuity Planning Methodology

To develop an efficient and effective business continuity plan, one must consider all the required planning issues, regardless of whether your organization is large or small. Major planning considerations, however, differ from one source to the next (Weems, 1999). Therefore, based on a study of various existing methodologies and each one's strong and weak points, a seven phase BCP methodology has been developed. These seven phases are as discussed below:

- **The project planning (PP) phase:** This phase incorporates all those activities required to ensure that the BCP project is properly planned.
- **The business impact analysis (BIA) phase:** During the BIA phase critical business processes are identified and then analyzed. Once the analysis is complete, the impact that various disasters may have on business should become clear (Gordon, 2000).
- **The business continuity strategies (BCS) phase:** This phase entails the identification of various strategies that focus on ensuring business continuity and recovery. It requires the review of the various identified disaster scenarios to develop methods to deal with these situations (Wilson, 2000).
- **The continuity strategies implementation (CSI) phase:** For each of the strategies defined in the business continuity strategies phase, detailed functional plans must be developed with which to respond to the various scenarios.
- **The continuity training (CTR) phase:** Business continuity training must form part of the organization's training framework and should be allocated part of the training budget. The training should be carried out as soon as the plan is complete as well as when it undergoes significant changes (Morwood, 1998).
- **The continuity testing (CTE) phase:** Testing is used to determine whether all the individual contingency plans are adequately written to ensure continuity of business

processes and the recovery of the data centre. (United States General Accounting Office, 1998).

- **The continuity plan maintenance (CPM) phase:** It is imperative that a business continuity plan is reviewed regularly and updated if required. This is done to ensure that the plan stays effective and up to date (BS7799-1, 1999)

Most of the above-discussed phases are scalable in such a way that they could be either entirely or partially implemented. The next section will discuss an implementation approach that could be utilised to simplify the implementation of BCP methodologies for small to medium sized organisations.

5. A Cyclic Approach to Methodology Implementation

As mentioned earlier, a few problems concerning known methodologies were identified. One of the most prominent, however, is the lack of implementation guidelines for BCP methodologies. The rest of this paper will, therefore, concentrate on addressing the problem of implementing a BCP methodology effectively. This will be done through the definition and a thorough discussion of the cyclic approach.

The concept of a cyclic approach will be introduced by means of an example. The idea behind this approach could be compared to building an outer city wall as have been done in medieval times. Building such a wall would obviously not be a simple task. If, for example, it was decided that the wall should be twenty feet high, building a twenty foot section along one part of the city at a time would be impractical and would offer no protection until the whole wall is completed. However, if the wall were to be built in phases, it would provide increasing levels of protection until the wall has been completed.

During the first phase, the wall could be built five feet high around the city. This would, for example, serve to keep out small predators threatening the livestock. The next phase would involve continuing the building process until the wall is ten feet high. At this height, the wall would succeed in keeping out the small predators as well as protecting against threats the five-foot wall did not cater for. Further improvements would include raising the wall to a height of fifteen feet and finally twenty feet. The twenty-foot wall will keep out the majority, if not all, of the anticipated threats. Each phase, therefore, builds on the previous by adding functionality to that which already existed.

The merits of such a phased approach are obvious. If the project is relatively large, but the workforce and funding are limited, it is advantageous to complete the project in various steps. An identical approach could be used towards the proposed BCP methodology implementation. It aims at dividing a methodology into four separate sections. Each section, or cycle as it is called in this approach, will have a different disaster recovery/business continuity related goal. It can be applied to most BCP related methodologies.

To illustrate the workings of the cyclic approach, the seven-phase BCP methodology discussed in the previous section will be used as a sample methodology. The following sub sections will discuss how this methodology has been split up to accommodate the cyclic approach, which is depicted in figure 2. The four cycles, in order, are the backup cycle, disaster recovery cycle, contingency planning cycle and business continuity planning

cycle. Some organisations may only require a backup plan, while others have to implement a full business continuity plan. The cyclic approach therefore provides one with the option to implement a methodology in four different stages where each stage is separate from the next.

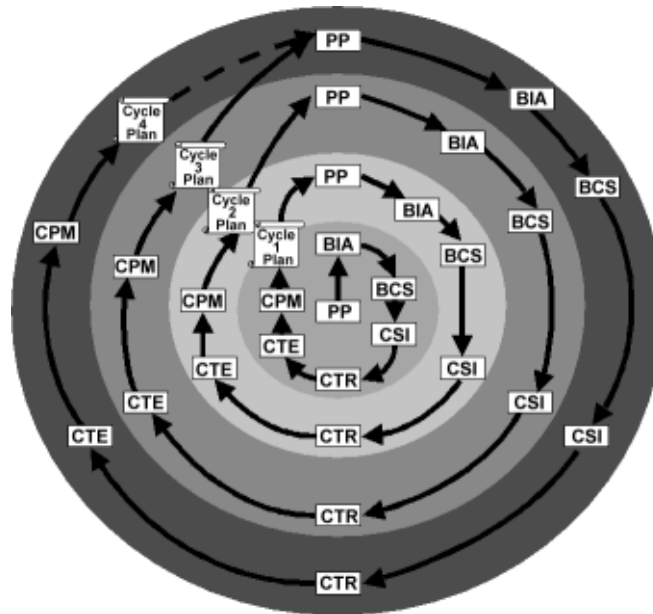


Figure 2: A cyclic approach to BCP

The backup cycle: If an organization has no access to their data after a disaster, it is virtually impossible to recover. Having an effective backup plan in place lays the foundation for further recovery efforts (Koski, K, 2001). For this reason the backup cycle has been chosen to initiate the implementation a BCP methodology. Although ensuring data backup and availability is the main purpose of this cycle, activities belonging to other methodology phases also need to be included. As this is the first cycle, it is essential that all project planning activities are carried out. Following the project planning is the performance of all BIA activities. As the organizational data is mostly identified during the BIA phase, all of the analysis activities need to be performed during this first cycle. Critical data then needs to be identified and it needs to be ensured that this data is continually available. This is achieved through regular backup and offsite storage of data.

Identification of the required teams to perform all backup cycle activities will be done during the strategies implementation phase. All that is left is training, testing and maintenance for this cycle. Training is fully carried out and will include both introductory and detailed awareness training. The topic for training should, however, only concentrate on backup cycle activities.

Testing should only include procedures to verify the efficiency of the backup plans. This will include attempting to determine whether all necessary data is backed up and whether it can be retrieved and restored within the time specified. After testing, plan maintenance should commence. Maintenance should be carried out in full irrespective of whether the continuity plan is merely a backup plan or a fully functional business continuity plan.

The disaster recovery cycle: The main objective of this cycle is ensuring that IT can recover effectively following a disaster. As for the first cycle, project planning activities

should once again be included as part of this cycle. It is imperative that management commitment is obtained before the second cycle commences. Employees and plan participants must furthermore be introduced to disaster recovery cycle concepts and schedules and milestones must be identified for the rest of the cycle. Having completed the project planning for the second cycle, it is time for the BIA again. All processes and supporting resources should already be identified and prioritised at this point. This eliminates the need for a further complete BIA. A brief review should, therefore, be sufficient to identify any changes in existing processes or the addition of new processes.

During the continuity strategies phase one usually identifies various recovery alternatives by assessing the recovery timeframes for the most critical business processes. This, along with the emergency response procedures and the recovery procedures written during the strategy implementation phase, must be completed. Furthermore, the teams responsible for the recovery efforts must be identified. To bring this cycle to a close, training testing and maintenance have to take place.

The contingency planning cycle: The contingency planning cycle aims at ensuring the continuity of all critical business processes while IT is recovering. Therefore, this cycle mainly concentrates on the identification of procedures to continue each business process, along with the steps supporting this. As have been the case in preceding cycles, planning is an essential activity that includes steps identical to the disaster recovery cycle. Management must support all decisions and a meeting to discuss this cycle with project participants must take place. Also, a BIA review should once again prove sufficient for this cycle. The difference between this cycle and the preceding one comes into play during the continuity strategies and strategy implementation phases. The user holding strategies, part of the continuity strategies phase, directly supports business continuity and is therefore included in this cycle.

Strategy implementation phase steps, such as process continuity procedures and team identification, will also form part of this cycle. Training, once again, will involve informing employees about business process continuity and other issues regarding the contingency planning cycle. Following the training, the testing phase as in the previous cycles, will concentrate not only assessing the effectiveness of plans for this cycle, but also those developed during the preceding cycles. Maintenance should be completed soon after testing to ensure that the entire plan stays up to date.

The continuity planning cycle: At this stage of the BCP project, the business continuity plan could be said to be nearing completion. This cycle will concentrate on business continuity as a whole, i.e. on both recovery and business process continuation. It mainly contains the various steps that could not be directly attributed to just continuity or recovery, but rather apply to all these previously established goals or related goals. The project planning section of this cycle is once again identical to the previous two cycles. As for preceding cycles, management is required to commit to decisions subject to the current cycle. A final orientation meeting is required to discuss cycle prospects and schedules.

A review of business processes is required to ensure information is correct and to record any new processes and related information added since the review done in the previous cycle. Progressing to the continuity strategies phase, activities that need to be completed are the insurance cover review, public relations preparation and emergency resources identification. Finally, before training, testing and maintenance commence, the remaining

group of teams responsible for activities during this cycle need to be identified. Training, testing and maintenance are conducted in the same fashion as before.

6. Conclusion

Information and IT have become a vital part of conducting business in our technologically advanced world. Undeniably a business can practically not do without these two components for extended periods of time. Employees, shareholders and customers have come to expect that information should be available around the clock. Even a minor disaster or disruption could cause irreversible damage to an organization and its public image.

To ensure that an organization could recover after a disaster, a complete business continuity plan should be in place. A complete BCP methodology should preferably be followed to ensure that such a plan is effective in protecting an organization. Such a methodology does not necessarily have to be different from those used in larger organisations. It does, however, need to be scalable. A large number of BCP methodologies are available, but it is rarely specified how each should be implemented. Once again, smaller companies might have to implement a methodology differently than larger organizations. For this reason a method simplifying the implementation process was developed.

As explained in the paper, the approach followed was to define a BCP methodology that is scalable to cater effectively for small to medium sized organisations. Furthermore, a cyclic implementation approach, utilising four distinct cycles, was proposed. Each cycle concentrated on a specific BCP goal and each goal was completed and tested before the next was started. With this implementation approach, an organisation could implement only that part of a methodology that suits their unique recovery requirements.

Further study will be aimed at the identification of methods to ensure that a business continuity plan is continually and dynamically maintained. This will guarantee that the plan stays up to date and thereby effectively caters for disasters at any time. This study will also concentrate on activities that will ensure that human involvement in BCP is maximized and by so doing increase employees' BCP awareness and readiness.

Reference List

- Barrow, C. (1993). The Essence of Small Business. Great Britain: Prentice Hall Inc.
- Beckmeyer, M. (2001). BCP at Small and Large Companies. Contingency Planning & Management. [Online]. [Cited October 19, 2002] Available from Internet URL http://www.contingencyplanning.com/article_index.cfm?article=379
- Bowler, A. & Dawood, M. S. (1995). Entrepreneurship and Small Business Management. Cape Town: Nasou
- BS7799-1. (1999). Information security management – Part 1: Code of practice for information security management. London: British Standards Institution
- Business Contingency Preparedness (2000). Glossary of Contingency Terms. [Online]. [Cited May 11, 2002] Available from Internet URL <http://www.businesscontingency.com/glossary/html/glossary.htm>
- Davenport, P. B. (1995). ISO 9000 In A Small, Vibrant Economy, With, Typically, Small To Medium Sized Businesses. SABS Bulletin, 14 (5), pp. 24-28
- Devargas, M. (1999). Survival is Not Compulsory: An Introduction to Business Continuity Planning. Computers & Security, 18 (1), pp. 35-46
- Edwards, B. (1994). Developing a Successful Network Disaster Recovery Plan. Information management & Computer Security, 2 (3), pp. 37-42
- Glenn, J. (2002). What Is Business Continuity Planning? How Does It Differ From Disaster Recovery Planning? Disaster Recovery Journal [Online]. [Cited May 11, 2002] Available from Internet URL <http://www.drj.com/articles/win02/1501-14p.html>
- Glorioso, R. M. & Desautels, R. E. (1999). Disaster Recovery or Disaster Tolerance: The choice is yours. Disaster Recovery Journal [Online]. [Cited November 21, 2000] Available from Internet URL <http://www.drj.com/articles/spr99/glor.htm>
- Gordon, C. (2000). How to Cost Justify a Business Continuation Plan to Management. Disaster Recovery Journal [Online]. [Cited March 7, 2002] Available from Internet URL <http://www.drj.com/articles/spring00/1302-05.html>
- Griffin, R. W. (1990). Management (3rd ed.). Boston: Houghton Mifflin Company
- Halliday, S., Badenhorst, K. & von Solms, R. (1996). A business approach to effective information technology risk analysis and management. Information Management and Computer Security, 4(1), pp. 19-31
- Hassim, M. (2000). To plan or not to plan? Accountancy SA [Online]. [Cited May 11, 2002] Available from Internet URL <http://www.accountancysa.org.za/archives/1999nov/features/plan.htm>

Hawkins, S. M., Yen, D. C. & Chou, D. C. (2000). Disaster recovery planning: a strategy for data security. Information Management and Computer Security, 8(5), pp. 222-229

IBM Global Services. (2000). Managing information technology in a new age [Online]. [Cited October 18, 2000] Available from Internet URL <http://www.ibm.com/services/whitepapers/gsw1178f.html>

Jackson, C. & Carey, M. (1997). Budgeting Basics. Contingency Planning & Management [Online] [Cited October 19, 2002] Available from Internet URL http://www.contingencyplanning.com/article_index.cfm?article=62

Johnson, J. (2002). Internal Auditing [Online]. [Cited October 31, 2002] Available from Internet URL <http://cobacourses.creighton.edu/fin402/Semester%20Projects/johnson.htm>

Koski, K. (2001). Backup and Offsite Vaulting [Online]. [Cited November 21, 2000] Available from Internet URL <http://w3.arcusds.com/Backup%20White%20Paper.pdf>

McAnally, P., DiMartini, B., Hakun, J., Lindman, G. & Parker, R. (2000). Real-time data availability solutions: Does your business have a need for speed? Disaster Resource Guide [Online]. [Cited May 11, 2001] Available from Internet URL http://www.disaster-resource.com/cgi-bin/article_search.cgi?id='22'

Megginson, W. L. (1994). Small business management: an entrepreneurs guide to success. United States of America: R.R Donnelley & Sons Company

Morwood, G. (1998). Business continuity: awareness and training programmes. Information Management & Computer Security, 6 (1), 28-32

Rubin, H. (May/June 1999). Bracing for Zero Day. IT Pro. pp.73-76
United States General Accounting Office. (1998). Year 2000 Computing Crisis: Business Continuity and Contingency Planning [Online]. [Cited October 23, 2000] Available from Internet URL <http://www.gao.gov/special.pubs/ai10119.pdf>

von Solms, R (1999). Information security management: why standards are important. Information Management and Computer Security, 7(1), pp. 50-57

Weems, T. L. (1999) Business Continuity Planning-for the rest of us. Disaster Recovery Journal [Online]. [Cited October 23, 2000] Available from Internet URL <http://www.drj.com/articles/fall99/weem.htm>

Wilson, B. (2000). Business Continuity Planning: A Necessity In The New E-Commerce Era. Disaster Recovery Journal [Online]. [Cited October 21, 2000] Available from Internet URL <http://www.drj.com/articles/fal00/1304-02.htm>