UNIVERSITY *of the*
WESTERN CAPE

An investigation into Business Continuity Plan (BCP) Failure during a Disaster Event

Mogamat Fadeel Sambo

Student Number: 2908157

Masters in Information Management (MCOM (IM))

Full Thesis

Supervisor: Dr Felix Bankole

Co-Supervisor: Dr Zoran Mitrovic

DECLARATION

Title of Master's Thesis: An Investigation into Business Continuity Plan (BCP) Failure during a Disaster Event.

I Mogamat Fadeel Sambo, declare that "An Investigation into Business Continuity Plan (BCP) Failure during a Disaster Event" is my own work, that it has not been submitted for any degree or examination at any other university, and that all the sources I have used or quoted have been indicated and acknowledged by complete references.

Name: Mogamat Fadeel Sambo

ABSTRACT

This thesis examines what a Business Continuity Plan (BCP) should comprise off, as well as the difference between a BCP and a Disaster Recovery Plan (DRP) and the key elements of an effective BCP as well as the different types of disasters. It also investigates why companies that have BCP in place and conducts testing of their plan on a regular basis, either quarterly or bi-annually, still experience prolonged downtime during a disaster resulting in Service Level Agreements (SLA) not being met or major financial loses. It also inspects acceptable processes within a BCP to determine whether there are ways of improving these processes to prevent companies from experiencing prolonged downtime.

The objective of this research is to determine and understand:

- Why organisations within the Western Cape experience prolonged downtimes during a disaster event
- The potential deficiencies in a BCP and how they can be amended.

A case study of four companies based in the Western Cape was conducted. These companies were chosen because each of them has a BCP in place and each have experienced prolonged downtime during a disaster. Qualitative interviews with the aid of an open-ended questionnaire were used to interview the BCP or Risk Manager of each company. The data was analysed to determine what the causes of their prolonged downtime were during a disaster. In the analysis and findings process each company is presented as a separate case study.

The intension with this research study is to add an additional concept to the Common BCP Process that was identified within this study and that formed the basis for the Conceptual Framework, thereby reducing the downtime during a disaster for the companies that formed part of the research.

ACKNOWLEDGEMENT

All thanks and praise is due to ALLAH who has given me the strength, patience and perseverance to continue with my studies.

- Professor Yusuf da Costa, my mentor, friend and most importantly my Sheikh, whose continuous subconscious voice has always reminded me to finish what I have started and inspired me to achieve more.

- Dr Zoran Mitrovic for being more than my co-supervisor; who has kept me motivated and focused on my goals and for continually believing in me.

- Dr Grafton Whyte, co-supervisor and friend who always inspired me and pushed me to give my best.

- Dr Felix Bankole, for being such a great supervisor and for his commitment. I have learnt so much from you, I thank you.

- My mother; Amina Sambo, who has always encouraged me and believed in me.

- My wife Nabewiya, whose unselfish acts of patience and perseverance has helped me to achieve what I am today. You are my soul mate and I thank you for being part of my life.

- My children: Adeel, Luqmaan, Rashieda and Nabeelah. Thank you for sacrificing your time with me so that I could reach my goal. I thank Allah for the family he has given me.

DEDICATION

This work is dedicated

to my parents

especially my father
(may Allah be pleased with him)

who was always there for me

and inspired me to further

my studies and

instilled in his children the value of education

LIST OF ACRONYMS

BCP (Business Continuity Plan)

BCM (Business Continuity Management)

BC (Business Continuity)

DRP (Disaster Recovery Plan)

DR (Disaster Recovery)

BIA (Business Impact Analysis)

RTO (Recovery Time Objective)

RPO (Recovery Point Objective)

MTD (Maximum Tolerable Downtime)

KEY WORDS

Business Continuity Plan, Business Continuity Management, Disaster Recovery Plan, Risk Management, Enterprise Risk Management, Disaster Risk Management.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

1.1 Introduction

Organizations today are entirely dependent on the availability of their Information Systems (IS) to run the daily operations to ensure competitive advantage and maximum return on investments. Systems disruptions or down-time can have a negative impact on the effectiveness and efficiency of doing business (Al-Zahrani, 2009).

The term, Business Continuity (BC) refers to the ability of a business to continue with its operations even if some sort of failure or disaster occurs (Bajgoric & Moon, 2009). Bajgoric & Moon (2009) further suggests that there are several factors affect the level of BC such as:

- data availability;
- application availability;
- networking reliability;
- operating system's reliability,
- availability and scalability and
- server hardware reliability,

A Business Continuity Plan (BCP) is an iterative process designed to identify business critical applications and endorse policies, procedures, processes and plans to ensure the continuation of these functions in the event of a disaster (Nicolette & Schmidt, 2001). Nicolette & Schmidt (2001) further states that each organization is unique and as such will have a unique BCP irrespective of similarities within industries and from company to company.

A BCP is also a document consisting of a collection of procedures and information which is developed and maintained to be used in the event of an emergency or disaster (Rozek & Groth, 2008). A BCP can also be considered as a process that ensures that operations and services are uninterrupted for the end-users and or customers (AT&T, 2002).

A disaster is thus not solely restricted to natural catastrophic events like the tsunamis and typhoons but may also include any event that may importantly affects the operation of an organization, such as human error in data entry, or intentional acts like the September 11disaster in 2001 (Chow & Ha, 2009).

A crisis or disaster could possibly be any emergency that suddenly occurs and that disrupts day to day operations of an organization or community, which could damage a company's competitive position, thereby requiring immediate attention (Phelps, 1986).

Natural disasters are not the only disasters, other aspects such as technological disasters, riots and human carnage and terrorisms have over the years played an equal if not larger share in creating disasters (Sayen, 2008).

A Disaster Recovery Plan (DRP) is a written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities (Swanson, Lynes & Gallup, 2010).

A DRP is a manual of instructions for individual people to perform specific tasks should a disaster occur (Edwards, 1994).

An executive at the infrastructure division of a company called UCS Solutions states that even though South African companies tend to be relatively strong in the field of Disaster Recovery and Planning (DRP), they are not as good at Business Continuity Planning (BCP) and that the approach is reactive rather than proactive (Harris, 2001).

The traditional DRP, which focuses on restoring the centralized data centre, might not be sufficient. A more comprehensive and rigorous BCP is needed to achieve a state of business continuity where critical systems and networks are continuously available (Planning, 2000).

Many businesses today require 24 hours and 7 days a week operations in order to survive. A single downtime might mean the difference between financial gain and financial loss. With the ever increasing dependency on Information Technology (IT) services in Small to Medium Enterprises (SME's) in South Africa; it has become a business requirement that systems be fully operational even during a disaster.

From the earthquakes and tsunamis that pounded Japan to the floods in Australia, the headlines this year have provided many examples of just how fragile IT infrastructures are in the face of disasters (Harris, 2001). Harris, (2001) further states that a few large South African companies, notably the banks and mining houses take business continuity seriously; many others regard it as a grudge purchase.

1.2 Background to the study

Working for SME's within the Western Cape I was fortunate to be part of their BCP and DR team. These companies religiously performed testing on their BCP and documents whenever a plan failed. At one of the companies where I was employed an incident took place. It was on a Friday at 07:00 that a mission critical server had crashed. This server held all the company's financial records and was used extensively by the Accounts, Human Resource and Payroll departments. When a server like this crashes it brings production for the afore-mentioned departments to a grinding halt. It took the database administrator, system administrator and two outsourced companies 11 hours (until 18:00) to repair the crashed server and recover the databases that resided on that server. The financial department and other administrators were unable to work online because there was no Fail-Over or Backup server available and as a result they had to perform some tasks manually. A disaster of this magnitude halted business processes and translated to huge losses as staff members had to work over the weekend to catch-up on the missed transactions.

I have experienced and witnessed similar incidents as to the one described above at various other companies whilst being employed there, which led me to research why companies that have BCP in place and perform regular testing still experience prolonged downtime following a disaster event.

1.3 Statement of research problem

Most companies within the Western Cape have a BCP in place, but still experience prolonged downtime during a disaster.

1.4 Research Questions

Based on the stated research problem the following questions have been identified:

1.4.1 Main Research Question

What are the causes of prolonged downtime during a disaster event and how are BCP implementation gaps addressed?

1.4.2 Research Sub-Questions

- What are the different types of disaster events?
- What are the key elements of an effective Business Continuity Plan?
- What are the factors that cause BCP failure?

1.5 Research Objectives

Linked to the research questions, the following research objectives were established:

- To identify why companies have prolonged downtime during a disaster.
- To compare BCP of companies with that of best practice and to identify any vital gaps
- To make recommendations for addressing BCP implementation gaps by adding a new model using the conceptual framework model that is based on common BCP processes.

1.6 Conceptual framework

A conceptual framework consists of statements that connect intellectual perceptions to realistic data. Conceptual frameworks are developed to describe abstract phenomena that occur within related or similar circumstances (Rudestam and Newton, 1992)

Important concepts namely Obtaining Management Approval, Performing Business Impact Analysis, Developing a BCP, Testing the BCP and Maintaining the BCP that were obtained from the literature review chapter in order to create a conceptual framework which will form the basis of this research. The different processes that harvested the concepts are the seven-step contingency planning process by

Swanson, Lynes & Gallup (2010), BCP Lifecycle by Al-Zahrani (2009) and a seven-phase BCP methodology that has been developed by Botha & Von Solms (2004).

1.7 Research Design and Methodology

This research adopted the case study approach within the qualitative research method. Four companies from within the Western Cape who each had BCP in place and had prolonged downtime during a disaster were selected. The risk manager from each company was interviewed and recorded. This method is useful when a small number of candidates are interviewed, which enabled the researcher to either write up a single case or explore themes shared between different cases (Fades, 2004).

1.8 Findings and Results

The data collected from the companies that formed part of the research was recorded, analysed and summarized in a tabular format to gauge commonality from the responses and to establish a pattern as to why each company experienced prolonged downtime during a disaster. It became evident that certain crucial aspects such as the network routers, network connections and software application services within their BCP has been overlooked and thus could not be implemented, causing them to have prolonged downtime during disasters.

1.9 Limitations of this study

The study is to determine why companies that have BCP in place and perform regular testing of their BCP, still experience prolonged downtime during a disaster. The research was limited to companies in the Western Cape. The main limitation is the limited sample size of 4 companies, which considerably limits generalisation of findings of this study.

Even though this research had a limited sample, it has both strong and weak points. The strength is that users could describe their lived experience in their own words which allowed the researcher to construct themes from users’ descriptions and interpreting the data. The weakness of this research is the limited sample.

1.10 Ethics Statement

This study followed the guidelines required for all research ethics. The research followed the qualitative stream thereby allowing me the privilege to interview participants who did not only give up their time, but gave honest testimony on how they felt about their experiences. The interviews took place at the offices of each of the respondents and interviews were conducted with either the BCP Manager or either IT Risk Manager. As each company requested to remain anonymous, the identities and designations of the interviewees have not been disclosed, and the data extrapolated was formulated to protect anonymity, and uphold the ethic of confidentiality.

1.11 Recommendations

This research aim at contributing either to

- Academic knowledge - Allowing academia to understand what a BCP should comprise of, the difference between a BCP and a DRP.
- Or to Business - To convince non IT directors and managers of the importance of a solid BCP as well as aiding them in compiling an effective BCP.

No doubt disasters will come and go, but will companies stand the test of time and live to tell the tale or will they too perish like the buildings in Japan, Indonesia, New Zealand, America and South Africa because of some inadequacy in their BCP?

In the next chapter we will look at key elements that contribute towards the success of BCP of scholars and professionals from around the world to understand and answer the research objective and questions.

CHAPTER 2: LITERATURE REVIEW

2.1 Business Continuity Plan (BCP)

The frequent community-wide disasters, as well as unusual disasters that corporations, institutions, municipalities and government agencies have suffered in the last dozen or so years, have revealed that planning for disaster recovery only is simply not enough. We must also plan for business continuity (Moore, 1995).

Disasters occur for a number of reasons, both routine and dramatic, and BCP must address every aspect of operations (Cervone, 2006).

BCPs were once the narrow focus of risk managers and continuity practitioners, but are now on the front pages of the business press and on the minds of the world. September 11 brought BCP successes and failures; by analysing what went wrong, companies can help prevent history from repeating itself (Grimaldi, 2008).

It is therefore important to ensure that the correct procedures, policies and plans are in place to protect an organisation’s IT infrastructure and data. The backup and restoration of company’s data are crucial for any organisation in order for a company to carry on with business as usual in the event of a disaster.

Although authors differ on the exact and clear difference between BCP, DRP and Contingency Planning (CP), the inter-relationship of these processes, 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 below. 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 (Botha & Von Solms, 2004).

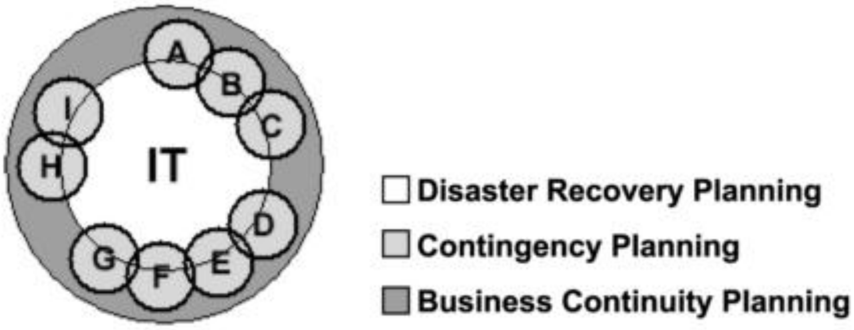

Figure 1: BCP, CP, DRP Relationship (Botha & Von Solms, 2004)

A BCP is an iterative process that is designed to identify mission critical business functions and enact policies, procedures, processes and plans to ensure the continuation of these functions in the event of unforeseen events. Even though there may be similarities within industries and from company to company, each organization is unique, and as such will have a unique BCP (Nickolette & Schmidt, 2001).

BCP is a collection of procedures and information which is developed, compiled and maintained in readiness for use in the event of an emergency or disaster, which would include the elements of a DRP (Rozek & Groth 2008). Rozek & Groth, (2008) further states that the process of creating, testing, and maintaining an organization-wide plan to recover from any form of disaster is called Business Continuity Planning

To completely define BCP one has to consider two aspects (Glenn, 2002).

1. It should be ensured that an organisation could continue business as usual, or on an acceptable level in the wake of disaster.
2. IT should be restored to a state similar to that before the disaster.

2.1.1. Benefits of a BCP

The goal of a BCP is to minimize operational risk in the face of a natural or man-made disruption. There are three key components to creating an effective BCP – people, infrastructure and processes (Campbell, 2012)

The aim of a BCP is to make provision for continuing business processes in a disaster situation while recovery is taking place (Glenn, 2002). Glenn (2002) also states that BCP is the process of investigating an organisation's critical functions, identifying the possible disaster scenarios and developing procedures to address these concerns.

BCP is an essential part of running any modern organization that takes its business and its clients seriously (Levinson, 2012). Therefore BCP could be considered as the safety net to clients.

BCP is both a management and an asset protection issue. The capacity to maintain business continuity or to regain it in a timely manner is the asset the plan protects, which is also good business sense by management (Heng, 1996).

In order to understand the benefits of BCP a snapshot of disaster impacts is presented. This information, as reported in the literature (Rothstein Associates, 2008), was compiled from multiple organizations worldwide:

- In Australia, businesses face threats from hurricanes, floods, etc. but about 55-60 per cent have no plan to cope with them.
- In a survey of the Chartered Management Institute in the UK, over half of the 1,257 managers surveyed had no business continuity plan in place.
- A total of 43 per cent of companies experiencing disasters never recover.
- A total of 90 per cent of businesses that lose data during a disaster will close their doors within two years of the event.
- Of businesses without a DR plan, 80 per cent close within 12 months of a flood or fire.
- Of companies that have a BCP plan, 43 per cent do not test it annually.
- More than 40 per cent of organizations do not have redundant servers or backup sites for critical business functions.

- A total of 66 per cent of US companies have not adopted or implemented US National Fire Protection Association (NFPA, 2007) standards on disaster/emergency management and business continuity.

The above statistics confirm that there is a need for raising BCP awareness.

2.1.2 BCP Challenges

According to the Government of Canada’s Public and Safety website lessons learned from the September 11disaster are as follows:

- plans must be updated and tested frequently;
- all types of threats must be considered;
- dependencies and interdependencies should be carefully analysed;
- key personnel may be unavailable;
- telecommunications are essential;
- alternate sites for IT backup should not be situated close to the primary site;
- employee support (counselling) is important;
- copies of plans should be stored at a secure off-site location;
- sizable security perimeters may surround the scene of incidents involving national security or law enforcement, and can impede personnel from returning to buildings;
- despite shortcomings, Business Continuity Plans in place pre September 11 were indispensable to the continuity effort;
- Increased uncertainty (following a high impact disruption such as terrorism) may lengthen time until operations are normalized.

The September 2001 attack on the World Trade Centre in New York City tested the contingency plans of American businesses to an unimagined degree. Companies that had business continuity plans in place were able to continue business at alternate sites with minimum downtime and minimum loss of data (Noakes-Fry, 2001). Noakes-Fry (2001) further iterates that in the aftermath of recent natural disasters, terrorism, and equipment breakdown, businesses have recognized more than ever the need for an organization to be prepared.

Difficult decision-making, for example a power failure, where it seems a total impact to the organization, but in reality such failures might not seem huge due to the nature of power failures that do not normally last long (Cervone, 2006). To iterate this point a company in the retail industry might experience a power failure at its head office, but this does not affect their day to day operations of their branches which are located throughout the country. Thus, decisions inside BCP to address this situation should concentrate on the deviation of normal situations such as what to do if power outage lasts for long time? Or what is the minimum acceptable time for recovery? Al-Zahrani (2009).

Companies are striving to meet the demand for continuous service and with the growth of e-commerce and other factors driving system availability expectations toward 24x365, the average organization's requirement for recovery time from a major system outage now ranges between two and 24 hours (Noakes-Fry, 2001).

Some companies will see the potential benefits for investing time in something that may never be required (Gardener 2010). Gardener (2010), while others may argue, or think differently, that:

- A BCP is planning for failure - effort should be focussed on preventing major incidents
- The major risks identified for the BCP are so unlikely they will never happen to us
- Their team is competent - they can cope with the known risks to our their business
- How can you have a BCP for the unexpected?
- Creating an effective BCP is too complex to achieve and to operate
- They already have an Emergency Response / Disaster Recovery Plan, therefore they don't need a new BCP
- Creating a BCP is a once-off project likely to be out of date or lost when required
- They are too busy and their priority needs to be elsewhere

2.1.3 Components of a BCP

A key component of a BCP is establishing the metrics of Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for data and applications which the IT department uses in creating their DRP and then to configure their backups and off-site replication (Langley, 2010). Langley, (2010) also mentions that the Recovery Time Objective (RTO) is the length of time that it takes to recover from an outage (scheduled, unscheduled, or disaster) and resume normal operations for an application or a set of applications.

The purpose of the BCP is to keep an organization's business running. This is accomplished by producing a plan that addresses the recovery of critical business functions in the event of a disaster (AL Zahrani, 2009).

The most important point to make about business continuity support technologies is that effectiveness depends entirely upon the organization's top-down commitment to the entire project, including the updating and testing which is necessary for maintenance (Noakes-Fry, 2001). He further states that even among corporations with business continuity plans, a KPMG study shows that less than one half meet an acceptable portion of their recovery objectives.

Table 1 below is a summary of key factors of a BCP as identified by Grimaldi (2008), Clifton (2000), Moore (1995), Heng (1996), Botha & Von Solms (2004), Ingenuity (2006) and Campbell (2012):

Table 1: Key Components of a BCP

Key Components	Author
Key components of an effective BCP are as follow: 1. Employ creative and customized thinking to the plan. 2. Test, test, and more test of the plan. 3. Keep the plan current – Update the plan as applications get updated 4. Get senior management involved and keep them committed.	(Grimaldi, 2008)

5. Establish a single person or group for enterprise-wide BCP coordination. 6. Include both business and technology units as active participants 7. Account for backup management 8. Maintain a financial commitment, even in times of cost reductions	
Before a plan can be tested, employers and employees need to be familiar with the content of the plan and their role in the response and recovery. This can be done by reading through the plan together and discussing how it could be applied to a fictional scenario.	(Clifton, 2000)
Issues that affect the plan are not only the physical recovery of the facility, but also: 1. emergency response plan; 2. emergency notification procedures; 3. emergency relocation procedures; 4. emergency access control and security; 5. emergency acquisitions and authorization; 6. emergency command centre requirements; 7. hot site – cold site – warm site requirements; 8. asset management and retrieval; 9. product and distribution recovery; 10. vital records recovery; 11. telecommunications recovery; 12. electronics recovery/restoration; 13. hazardous contamination; 14. environmental compliance; 15. health and safety issues; 16. Insurance loss documentation.	(Moore, 1995)
The primary component of BCP is to protect an organization when all or part of its operations or IT services are rendered	(Heng, 1996)

unusable. Detailed purposes are to: 1. provide for the safety and wellbeing of people in the branch at the time of the disaster; 2. establish management succession and emergency powers; 3. identify critical businesses and supporting functions; 4. minimize immediate damage and losses; 5. resume critical business functions in temporary premises; **6.** Return to normal operations when the primary facility is restored.	
To develop an efficient and effective business continuity plan, one must consider all the required planning issues	(Botha & Von Solms, 2004)
A high level of the Business Continuity Plan should include adequate coverage of the following elements: • Emergency response procedures - applies to any incident or activity that may endanger lives, property, or the ability to perform essential functions. • Arrangements, procedures, and responsibilities, including data backup, offsite storage and contingency safeguards, to ensure that operations can be continued if normal processing or data communications are interrupted for any reason for an unacceptable period of time. • Recovery procedures and responsibilities - to facilitate the rapid restoration of normal operations at a secondary site, following destruction, major damage or other interruptions at the primary site. • Minimally acceptable prioritized level of degraded operation of critical systems or functions. The business continuity plan must accommodate these established priorities. • Interim manual processes to enable the continuance of	(Ingenuity, 2006)

critical operations in the absence of application, operational and general IT support.	
There are three key factors to creating an effective BCP – people, infrastructure and processes. Other points that also responsible for an effective BCP are: • Identifying recovery point objectives (RPO) and recovery time objectives (RTO), making sure data protection solutions can meet these requirements. • Ensure that data protection isn't confined to premises. Having the backup at the same location as the systems does not help if the location is destroyed. • Prioritize off-site backup. Electronically keep a version of the environment at a contingency location and replicate system data onto it. If a full-time contingency location is lacking, or there is no bandwidth to electronically move information, keep backup data off-site physically with disks or tapes.	(Campbell, 2012)

Business continuity depends on the availability of critical elements such as operating systems, applications, databases and files that can seriously affect a company's ability to resume and continue its business (Moore, 1995).

Every BCP strategy includes three fundamental components: risk assessment, contingency planning, and the actual disaster recovery process (Rozek & Groth, 2008). BCP should encompass every type of business interruption -- from the slightest two-second power outage or spike up to the worst possible natural disaster or terrorist attack. In order for a plan to succeed, there must be multiple agency cooperation and involvement.

By upholding these key factors in the foreground of the planning process successful BCP will be ensured. A properly funded, well-prioritized continuity plan, combined with a regular programme of testing and disaster recovery drills, will help to safeguard an organization.

2.1.4 The BCP Process

A requirement of the BCP process is to instigate a “risk reduction programme”. This will ensure that company threats are identified and assessed accordingly (Karakasidis, 1997). Karakasidis, (1997) is further of the opinion that a BCP process should comprise of certain components and should be used in conjunction with a risk management process, i.e. a risk reduction programme should consist of the following points (Karakasidis, 1997):

1. Obtain top management approval and support.
2. Establish a business continuity planning (BCP) committee.
3. Perform a business impact analyses.
4. Evaluate critical needs and prioritize business requirements.
5. Determine the business continuity strategy and associated recovery process.
6. Prepare the business continuity strategy and its implementation plan for executive management approval.
7. Prepare business recovery plan templates and utilities, finalize data collection and organize/develop the business recovery procedures.
8. Develop the testing criteria and procedures.
9. Test the business recovery process and evaluate test results.
10. Develop/review service level agreement(s) (SLAs).
11. Update/revise the business recovery procedures and templates.

The term, business continuity or business continuance or business resilience refers to the ability of a business to continue with its operations even if some sort of failure or disaster should occur (Bajgoric & Moon, 2009). Bajgoric & Moon, (2009) states that there are several factors affect the level of BC such as data application and networking availability as well as the operating system’s reliability, availability and scalability and server hardware reliability affect levels of BC in organizations.

Design, installation and management of enterprise information systems are becoming a basic infra-structure and operation necessity in every organization and business sector and organizations are realizing the competitive advantage which Information Systems (IS) offer to them and the importance of which IS has on their daily operations (Chow, 2000). Chow, (2000) highlights the following considerations such as top management commitment, adequate budget and financial support, alignment of BCP objectives with organizations goals, adoption of project management techniques when developing BCP, the presence of a formal recovery/continuity planning committee and participation in BCP from each department in the organization.

The below seven-step contingency planning process that an organization may apply to develop and maintain a viable contingency planning program for their information systems (Swanson, Lynes & Gallup, 2010) These seven progressive steps are designed to be integrated into each stage of the system development life cycle (Swanson, Lynes & Gallup, 2010).

1. Develop the contingency planning policy statement. A formal policy provides the authority and guidance necessary to develop an effective contingency plan.
2. Conduct the business impact analysis (BIA). The BIA helps identify and prioritize information systems and components critical to supporting the organization’s mission/business functions. A template for developing the BIA is provided to assist the user.
3. Identify preventive controls. Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.
4. Create contingency strategies. Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.
5. Develop an information system contingency plan. The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system’s security impact level and recovery requirements.
6. Ensure plan testing, training, and exercises. Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.

7. Ensure plan maintenance. The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.

   Below in figure 2 is a summary of the seven-step contingency planning process

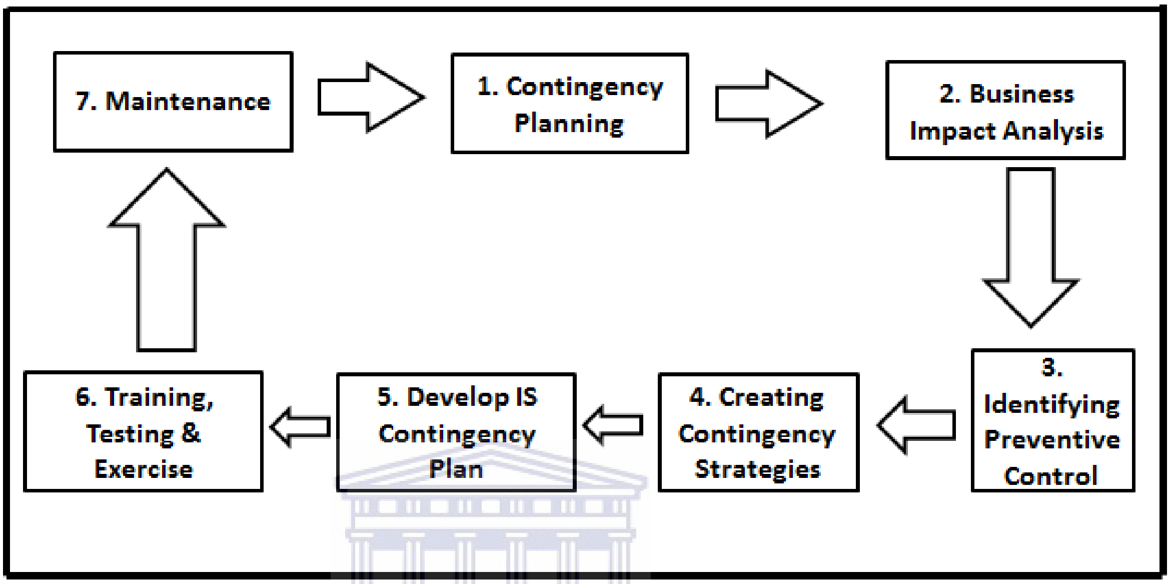
7. Maintenance
1. Contingency Planning
2. Business Impact Analysis
3. Identifying Preventive Control
4. Creating Contingency Strategies
5. Develop IS Contingency Plan
6. Training, Testing & Exercise

Figure 2: seven-step contingency planning process (Swanson, Lynes & Gallup, 2010)

Creating and maintaining a workable BCP is an essential factor in ensuring your organization's continued survival and prosperity (Rozek & Groth, 2008). According to Rozek & Groth, (2008), there are five main steps in the BCP process, namely:

1. **Initiation** - Prepare for the Initial Meeting with Senior Management, know as much as possible about the issues associated with the development of disaster planning.
2. **Business Impact Analysis (BIA)** – Prepare a BIA Questionnaire. The BIA is intended to help understand the degree of potential loss (and other undesirable effects) which could occur. This will cover not just direct financial loss, but many other issues, such as loss of customer confidence, reputation damage, regulatory effects, and so on.
3. **Disaster Readiness Strategies** - Define and Cost Business Continuity Alternatives. Using the information from the BIA, the project team should evaluate the alternative strategies that are available to the organization

4. **Develop and Implement the Plan** - Define the Scope and draw up a Business Continuity Plan. The plan may consist of:
    - 4.1. Multiple physical locations over broad geographic areas
    - 4.2. Various operations or departments at each location
    - 4.3. Business operations, processes or functions that require multiple agency cooperation to succeed
    - 4.4. Information technology ranging from desktop personal computers to inter-connected LANs to secure work resources to multi-server data centres, etc.
    - 4.5. Telecommunications (data, voice, video, multimedia, etc.) serving all internal locations and key client locations
5. **Maintenance and Testing** - Establish a Plan Exercise Program. Develop and conduct plan exercises. Exercises will grow in complexity over time. Include announced and unannounced events as well as scheduled and unscheduled tests.

A corporate business recovery plan needs to be “all things to all men”. It should be a plan which provides a high-level communications strategy for senior management, as well as the technical detail necessary to restore a critical process or application (Maslen, 1996).

The most common model of a BCP lifecycle in literature is shown below in Figure 4 and has four major phases (Al-Zahrani, 2009):

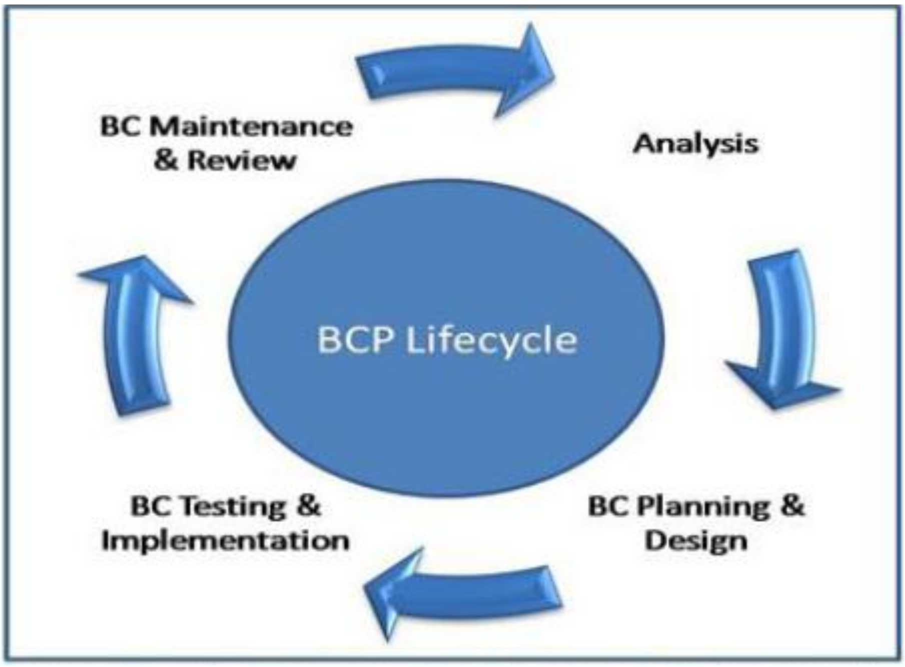

Figure 3: BCP Lifecycle (adopted from British Standards for BC www.bs25999.net)

Based on figure 3 above the four major phases are as follow (Al-Zahrani, 2009):

- **Analysis** – all business processes and functions are analysed by performing risk assessments and business impact analysis (Pit & Goyal, 2004). Business dependencies will be clear after completing this phase and can be visualized by Business modelling (Erlanger, 2006). The analysis phase identifies key requirement for the subsequent BCP phases.
- **BCP Planning and Design** – Activities in this phase include defining the scope and objectives of the plans, creating emergency procedures and the design of recovery solutions and procedures, as well as estimating costs and resources of developing the organization BCP (Pit & Goyal, 2004).
- **BCP Testing and Implementation** – the key activities in this phase include testing and deployment of plans and solutions and training of involved staff (Botha & Von Solms, 2004).
- **BCP Maintenance and Review** – regular review and enhancement as well as documentation will ensure that the plan is up to date (Botha & Von Solms, 2004).

The proposition in Figure 4 below shows that benefits will only arise if there is a business continuity linkage from Board right down to shop floor. Figure 5 below is based on Masaaki Imai's ends means chart for Kaisen (Imai,1986), shows how the methods adopted to meet aims at one level in an organisation become the aims at the next level down.

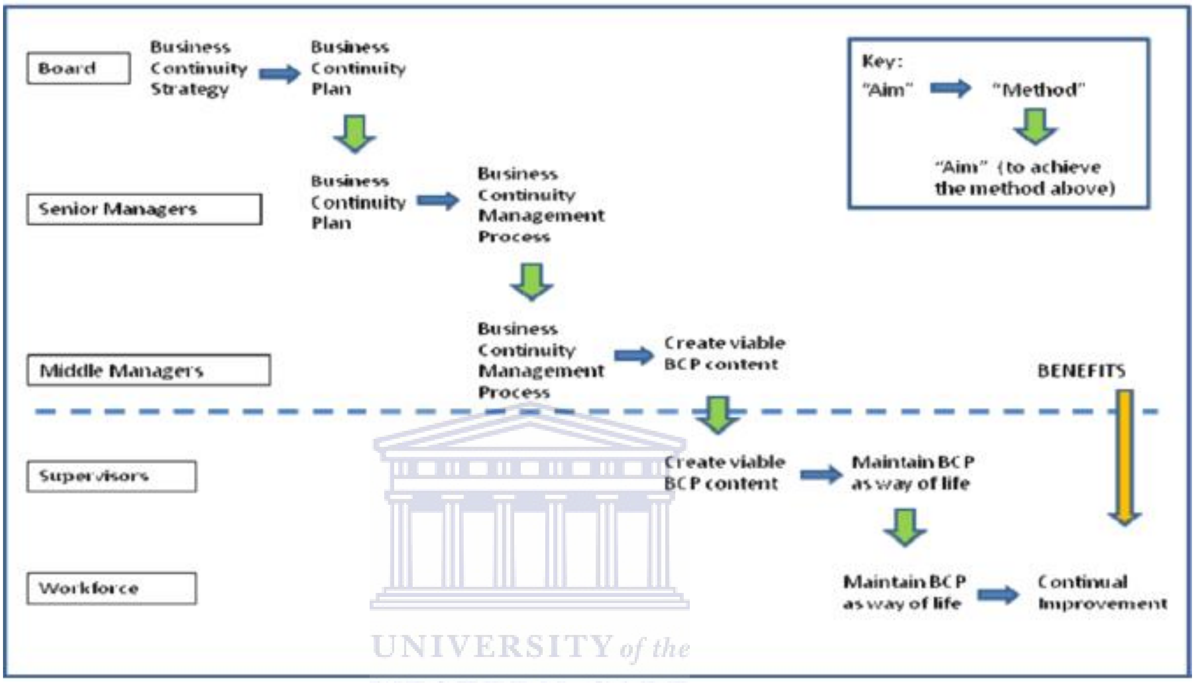
Board
Business Continuity Strategy
Business Continuity Plan
Key:
"Aim"
"Method"
"Aim" (to achieve the method above)
Senior Managers
Business Continuity Plan
Business Continuity Management Process
Middle Managers
Business Continuity Management Process
Create viable BCP content
BENEFITS
Supervisors
Create viable BCP content
Maintain BCP as way of life
Workforce
Maintain BCP as way of life
Continual Improvement

Figure 4: Strategy developed by Aims and Methods

It is noted that most BCP methodologies are variations of the classical project management methodology as BCPs require similar traits to those required in managing any other project (Heng, 1996). From this approach, many practitioners have developed their methodologies based on their own perspectives and the needs of their organization. The Standard Chartered Bank's BCP methodology is shown in Figure 5.

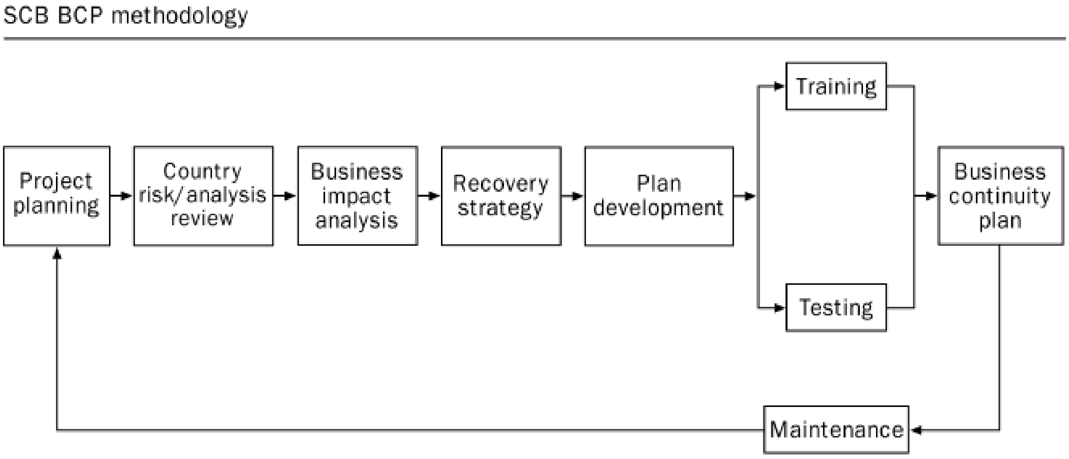

Figure 5: Standard Chartered Bank's BCP methodology (Heng, 1996)

The "plan" that results from the BCP is important; however the most important part is the process of creating the plan (Savage, 2002). Savage, (2002) further states that the process should include activities such as:

- Business risk and impact analysis
- Documenting activities necessary to prepare the organization for possible emergencies
- Identifying and authorising detailed activities for any disaster recovery phase
- Identifying and authorising detailed activities for managing the business recovery process
- Testing and auditing the business recovery process
- Implementing the process for keeping the plan up to date

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 Botha & Von Solms (2004). These seven phases are as discussed below:

1. The project planning (PP) phase. This phase incorporates all those activities required to ensure that the BCP project is properly planned.
2. The Business Impact Analysis (BIA) phase. During the BIA phase critical business processes are identified and then analysed. Once the analysis is complete, the impact that various disasters may have on business should become clear (Gordon, 2000).

3. 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).
4. 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.
5. 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).
6. 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).
7. 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 (BSI, 1999).

Most of the above-discussed phases are scalable in such a way that they could be either entirely or partially implemented. Figure 6 below is a summary of the above phase.

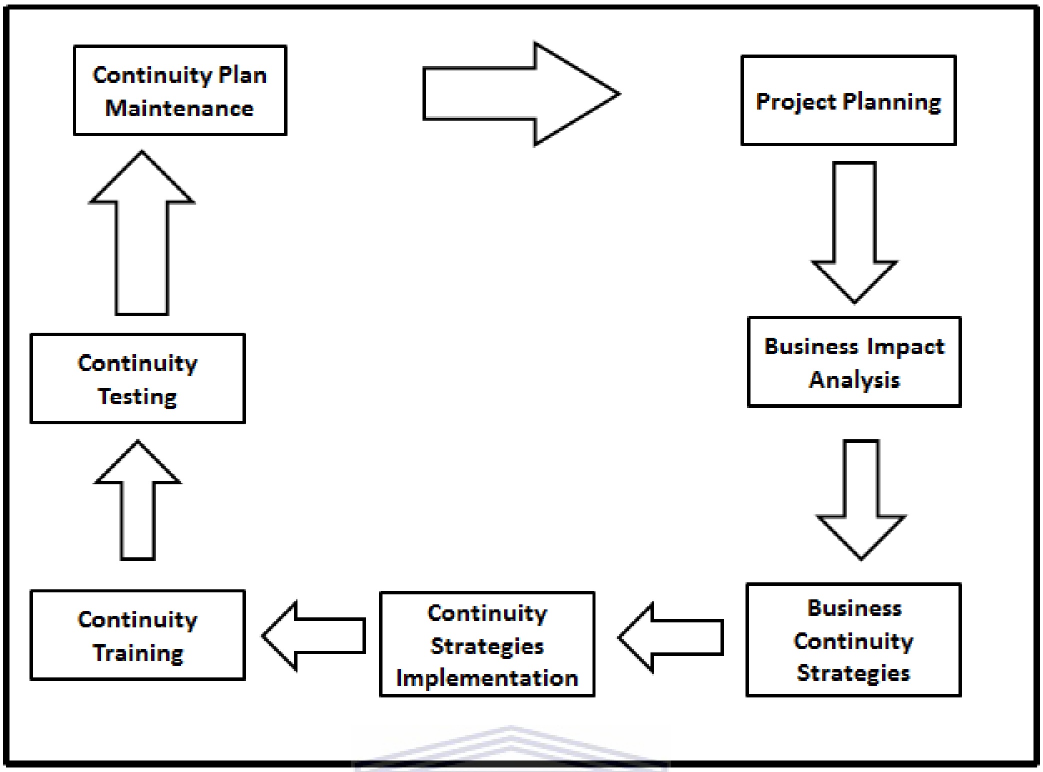
Continuity Plan Maintenance
Project Planning
Business Impact Analysis
Continuity Testing
Business Continuity Strategies
Continuity Strategies Implementation
Continuity Training

Figure 6: Seven-phase BCP methodology (Botha & Von Solms, 2004)

Botha and Von Solms went further to create a cyclic approach to BCP. To illustrate the workings of the cyclic approach, the seven-phase BCP methodology in figure 6 above was only the bases for the cyclic approach.

In figure 9 below 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 (Botha & Von Solms, 2004). The 4 Cycle Plan is as follow:

1. The back-up cycle - The backup cycle is to initiate the execution a BCP methodology. The main purpose of this cycle is to ensure that data is backed up and available.
2. The disaster recovery cycle - The main objective of this cycle is to ensure that IT can recover effectively after a disaster.
3. The contingency planning cycle - This step aims at safeguarding the continuity of all critical business processes while IT is in the process of

recovering. This cycle therefore mainly concentrates on the identification of procedures to continue each business process, along with the steps supporting this.

4. The continuity planning cycle - This cycle concentrate on business continuity as a whole, i.e. on both recovery and business process continuation.

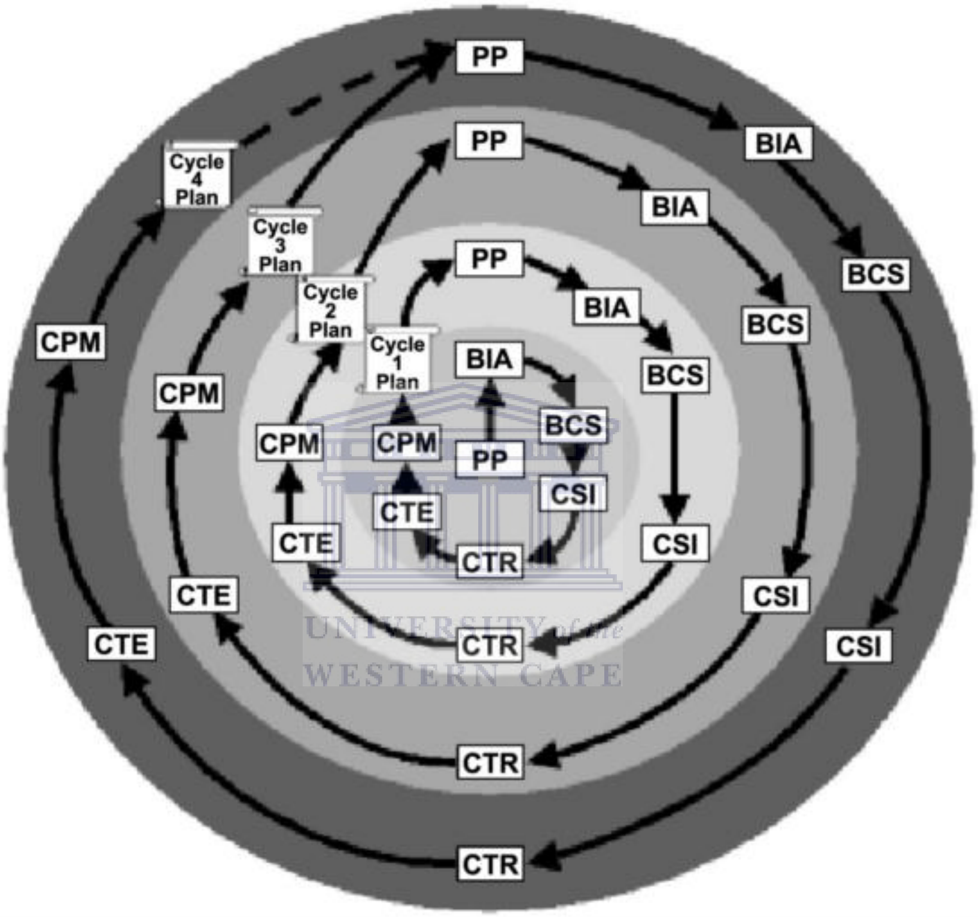

Figure 7: A Cyclic approach to BCP (Botha & Von Solms, 2004)

There are several BCP processes and models from (Karaksidis, 1997; Hinks, 2001; Heng, 1996; Varcoe, 1998; DRI international, 1998), which formed some common steps (Pitt & Goyal, 2004). These steps are:

1. Project Initiation – Obtain top management approval and support
2. Business Impact Analysis (BIA) – gathering of data and evaluating critical aspects that are core to the business.
3. Design and development of a BCP, which consist of administration procedures, forming a business continuity committee and BCP budgets

4. Creating a BCP. This point addresses emergency response procedures and control centre.
5. Testing the plan by having exercise programmes, scenarios and objectives.
6. Maintaining and updating the plan after failed tests and including those steps into the plan

To ensure that an organization could recover after a disaster, a complete BCP 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.

Based on the literature in this section, the table below summarizes the various BCP Processes.

Table 2: Summary of BCP Processes with reference to the Authors

Processes within a BCP	**Author**
1. Obtain top management approval. 2. Establish a BCP committee. 3. Perform BIA 4. Evaluate critical needs and prioritize business requirements. 5. Determine the business continuity strategy and associated recovery process. 6. Prepare business continuity strategy 7. Prepare business recovery plan 8. Develop the testing criteria 9. Test the business recovery process 10. Develop/review SLAs. 11. Update/revise the business recovery procedures	(Karakasidis, 1997)
1. Top management commitment 2. Adequate budget and financial support 3. Alignment of BCP objectives with organizations goals.	(Chow, 2000)

4. Adoption of project management techniques when developing BCP 5. Form a continuity planning committee. 6. Participation in BCP	
1. Develop the contingency planning policy statement. 2. Conduct a BIA. 3. Identify preventive controls. 4. Create contingency strategies. 5. Develop an information system contingency plan. 6. Ensure plan testing, training, and exercises. 7. Ensure plan maintenance.	(Swanson, Lynes & Gallup, 2010)
1. Initiation – Get Top Management approval 2. BIA 3. Disaster Readiness Strategies 4. Develop and Implement the Plan 5. Maintenance and Testing	(Rozek & Groth, 2008)
1. The project planning (PP) phase 2. The BIA phase 3. The Business Continuity Strategies (BCS) phase 4. The Continuity Strategies Implementation (CSI) phase 5. The Continuity Training (CTR) phase 6. The Continuity Testing (CTE) phase 7. The continuity plan maintenance (CPM) phase	(Botha & Von Solms, 2004)
1. Analysis 2. BCP Planning and Design 3. BCP Testing and Implementation 4. BCP Maintenance and Review	(Al-Zahrani, 2009)
1. BIA 2. Documenting activities for emergencies 3. Identifying and authorising events for any disaster recovery phase 4. Identifying and authorising activities for managing the business recovery process	(Savage, 2002).

5. Testing the business recovery process 6. Implementing & Maintaining the process	
1. Project Initiation – Obtain top management approval 2. BIA 3. Design and develop of a BCP 4. Creating a BCP. 5. Testing the plan 6. Maintaining and updating the plan	(Pitt & Goyal, 2004)

By examining the above table, certain steps within the BCP process are common amongst the various authors. These steps are:

1. Top management commitment – Chow, Karakasidis, Rozek & Groth, Pitt & Goyal feel that this is an important aspect.
2. Conduct a Business Impact Analysis (BIA) – this is agreed by all the authors in the above table except for Chow.
3. Develop a plan - Chow, Rozek & Goreth, Pitt & Goyal and Al-Zahrani all concur that this is an important part of a BCP.
4. Testing the plan - Botha & Von Solms, Chow, Swanson, Lynes & Gallup, Rozek & Groth, Karakasidis, Pitt & Goyal, Savage and Al-Zahrani agree that this is a crucial part within an effective BCP.
5. Maintaining the plan – this is agreed by Botha & Von Solms, Chow, Swanson, Lynes & Gallup, Rozek & Groth, Karakasidis, Savage, Pitt & Goyal and Al-Zahrani

Based on the above a common BCP Process model that would include the common steps within the BCP Process would be represented in the figure below. This model will also be used as the conceptual model.

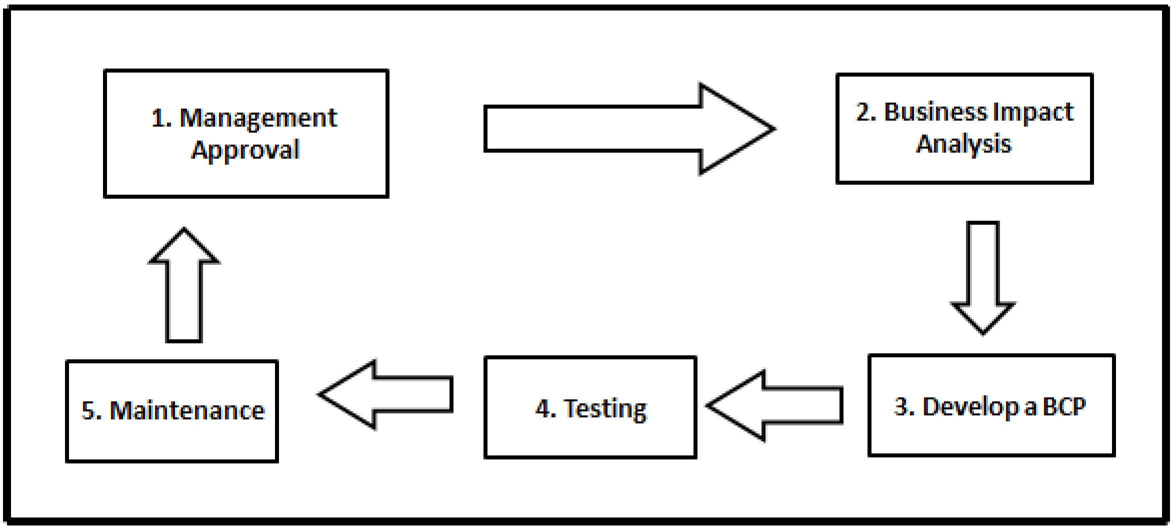

Figure 8 Common BCP Process Model

2.1.5 BCP Critical Success Factors

There are certain factors that are pertinent for any BCP, thereby allowing any company that has these factors in their BCP to have a faster recovery time than those who don't. One of the biggest challenges in BCP is identifying and protecting key essential factors.

Where a BCP has been established, its focus has largely been on Information Technology (IT) and not on taking into account other factors of the organisation such as people, the process and the infrastructure (Hearnden, 1995). In addition Hearnden, (1995) also highlights that where the plan is implemented only a few are tested and reviewed on a regular basis, thereby seriously undermining the effectiveness of the plan.

The table demonstrates the factors that causes BCP failure as per author

Table 3: Factors that causes BCP failure

Factors that cause BCP failure	Author
There are eight points of BCP failure: 1. A one-size-fits-all solution. The traditional one-size-fits-all solution typically relies on small recovery teams—often 20 % of staff—for a short period of time or requires clustering leadership in single sites to achieve economies of scale.	(Grimaldi, 2008)

2. Deficiencies in the tests. Organizations that spend the time, effort and expense to construct BCPs but do not test them are not managing their investments wisely. Most likely, these firms will not be able to successfully enact their BCPs when a crisis begins. 3. Inadequate maintenance. To prepare for a roadside emergency means more than carrying a spare tyre; it means checking the tyre regularly to make sure it is inflated. The same holds true for BCPs. Without adequate and aggressive maintenance, BCPs become quickly obsolete. 4. Lack of senior management involvement. A BCP project will not get off the ground without backing from the company leaders. The tone from the top can eliminate resistance to the tedious tasks of building, testing and maintaining BCPs. 5. No enterprise-wide accountability and coordination. A lack of centralized accountability creates varying levels of preparedness among divisions, putting the entire organization at risk. Organizations must establish a visible and prominent unit to coordinate the enterprise-wide BCP. Whether in the form of a project management office or a department with a full-time senior manager and support staff. 6. Operations take a backseat to technology. When the BCP is a technical project rather than a business-wide initiative, it becomes confused with a disaster recovery plan (DRP). Technologists hired as experts for DRPs often	

do not understand the nuances and risks involved in managing a business—and such an understanding is imperative when designing a BCP. When developing a BCP, the placement of technology first results in an ineffective plan. The plan will address technology issues but neglect human resources- and business process-related matters that are crucial for normal operations when business is interrupted. 7. No clear leadership structure or management contingency plans. Just as a BCP relies on the redundancy of data collection, the skills and knowledge of the staff must also be backed up. 8. Rash cost-reduction campaigns that eliminate the BCP. In today's economy, every organization is cutting expenses and looking to bolster its bottom line. Typically, the first places to look for rightsizing are support services or overhead units. By definition, BCP is not a revenue-producing area. At best, the most progressive organizations view it as revenue protection. Therefore, companies forced to shed expenses often slash funding for BCP initiatives. These companies are gambling that the financial gains of cutting overhead outweigh the heightened risk of not having the protection, at least for the short term.	
There are ten factors that will lead to BCP failure: 1. Failure to identify every potential event that can jeopardize the infrastructure and data from viruses to region that is prone to earthquakes and tornados. 2. Failure to cross-train personnel in disaster	(Molinari, 2010)

recovery and business continuity processes. Often businesses create Business Continuity plan that depends on just a few people and fail to identify and cross-train a pool of employees that are capable of responding in an emergency. 3. Failure to create alternative communication processes when your primary communication infrastructure is lost. 4. Failure to have adequate backup power - ensure that generators and power supply units are serviced and maintained. 5. Failure to know which resources need to be restored first. – Try to install mission critical applications that will allow most of parts of your business to operational. 6. Failure to have adequate physical documentation of your Business Continuity plan. Ensure that every process is well documented and describe the location of all system resources needed to accomplish the recovery. 7. Failure to validate the adequacy of your backups. Perform backups and restores regular intervals to test integrity of the backups. 8. Failure to test your Business Continuity plan. Schedule and unscheduled tests from basic power failures to catastrophic events has to be perform, so that those involve are familiar with the drill. 9. Failure to have passwords available to the Business Continuity team. Passwords need to be stored in at least two separate geographically, secure locations and ensure	

that more than one IT personnel has access to all passwords and codes. 10. Failure to keep your Business Continuity plan up to date. A BCP needs to be updated as business include new applications in there day to day running's.	
After the September 2001 attack on the World Trade Centre most companies were not able to recover after a disaster as most of the key players were not available	Noakes-Fry (2001)
Top five ways to fail at Business Continuity 1. Failing to understand the business. Not knowing the business processes and to identify business critical applications can cause delays in the restore process. 2. Executing methodology instead of managing a program – Most companies' purchase BCP tools which allow them to calculate the BIA based on questions asked to various business owners. The planning tool provides both an embedded methodology and a set of templates to assist in the planning efforts. In the event of a disaster they should follow what the toll recommended and not a methodology. 3. Unnecessarily using Business Continuity Jargon – Keep it simple and avoid using acronyms 4. Unrealistic Recovery Objectives 5. Failing to Create a Culture of Business Continuity	(Hutton & Rupert, 2009)

A comprehensive BCP that takes the above into consideration will dramatically improves a company's recoverable time and reduce the impact of any business interruptions.

2.1.6 Cloud adoption enabling BCP

Cloud computing is one of the most current and innovative technologies used to centralised information systems and infrastructure (Nichal and Mathur, 2010). Many organizations use cloud computing to store large volume of data at central location (Hudic et al., 2013).

According to Zainab, et al., (2013) the key benefits cloud computing is:

- To reduce the total cost of ownership and maintenance of IS
- Financial constraints of infrastructure maintenance and upgrade.
- Scalability of the system in both accessibility and availability.
- Scalability of storage capacity.

Hudic et al, (2013) further iterates that due to the ability of cloud computing to provide a wide range of reliable and cost-effective services, have encourage businesses to move their data or parts of it into the cloud. The adoption of cloud computing as a service has positively impacted the development of BCP/DRP from a process and risk perspective.

2.2 Disaster Recovery Plan (DRP)

In many organisations the DRP process starts somewhere in the middle of the organization and focuses narrowly on a given area (Phelps, 1986).

A DRP is a written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities (Swanson, Lynes & Gallup, 2010). The overall DRP plan should include at least the basic modules that will render it functional. These are: business impact analysis (BIA), risk assessment (RA), strategy definition, DRP, test and training of the plan, maintenance of the plan and certification of the plan (Aggelinos & Katsikas, 2011). DRP is about defining consistent, pre-planned actions that will react to various disaster scenarios and is about reacting to the disaster scenario after it has happened (Rosenberg, 2010).

2.2.1 Benefits of a DRP

The benefits of developing a DRP are according to Hawkins, Yen & Chou, (2000) that it eliminates any confusion and error in what should be done in the event of a disaster. It also reduces downtime to business, provides alternatives during a disaster, reduces the reliance on certain key individuals, protects the data of the organization, ensures the safety of company personnel, assist in an organized recovery

2.2.2 Components of a DRP

The components for a DRP according to Francen (2009) are to account for all six stages of the disaster recovery cycle namely normal operations, disaster events, disrupted operations, disaster restoration, the reconstitution process and the lessons that were learnt. DRP components would also involve the business to sign off on funding, planning groups and BIA, as well as to define the scope and objectives of the DRP, understanding the various systems and their dependencies, offsite data storage, support of data, ensuring continuous updates to the DRP, using a checklist to ensure that all servers and systems are backed up, continuous testing of the DRP and to ensure that the DRP plans are stored offsite (Francen, 2009).

2.2.3 The DRP Process

The process and strategies for developing a disaster recovery plan as suggested by Hawkins, Yen & Chou (2000) are as follows:

- **Perform a risk assessment** by checking inventory of the organization and identifying the systems and resources that are most critical to their business operations.
- **Identify possible vulnerabilities** will prevent a problem before it occurs.
- **Developing a plan of action** would be either by having a brainstorming session between management and corporate employees or by having each department develops their own recovery plan that will provide direction on how to quickly resolve a crisis.
- **Choosing an alternate recovery site** would be dependent on the type of disaster, for example a flood, power failure, fire and so on.

- **Selecting a backup strategy** could speed up the disaster recovery process. The two main effective backup strategies are the in-house backup system and off-site backup system.
- **Conducting a verbal walk-through** is mainly for employees who participate in the recovery process and discuss various “what if” situations.
- **Testing the plan on a regular basis to ensure its integrity** is important to any company as this is when the plan is updated.

Even though BCP and DRP seem similar, there are various definitions proving otherwise.

2.3 Difference between BCP & DRP

The term “Disaster Recovery” and “Business Continuity” are often used interchangeably; however they are in fact different but with complimentary components (Nickolette & Schmidt, 2001).

A DRP may support a BCP or COOP plan by recovering supporting systems for mission/business functions or mission essential functions at an alternate location. The DRP only addresses information system disruptions that require relocation (Swanson, Lynes & Gallup, 2010).

A BCP manual must be realistic and easy to use during a crisis. As such, BCP sits alongside crisis management and disaster recovery planning and is a part of an organization's overall risk (Clifton, 2000)

The table below is a clear illustration as to the difference between BCP and DRP

Table 4: Difference between BCP and DRP

Business Continuity Plan	Disaster Recovery Plan	Authors
Determine which	Recovery of systems and	(Nickolette & Schmidt,

business components and functions need to be recovered and which to ignore.	infrastructure components	2001)
A process of developing and documenting arrangements and procedures that enable an organization to respond to an event that lasts for an unacceptable period of time and return to performing its critical functions after an interruption	A document that defines the resources, actions, tasks and data required to manage the technology recovery effort. This is a component of the Business Continuity Management Program	(Hellman & Magnus, 2008)
BCP is concerned with the recovery and resumption of activities across the entire organization and is driven by senior management.	DRP primarily focused on the recovery of IT systems and applications and is driven by the IT department.	(Cervone, 2006)
BCP focuses on sustaining an organization’s mission/business functions during and after a disruption and may be written for mission/business functions that address the entire organization’s processes.	DRP is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency.	(Swanson, Lynes & Gallup, 2010)

A business recovery plan is a document used to assist organizations in recovering its business functions	A disaster recovery plan is however a document design to assist an organization in recovering from data losses and restoring	(Hawkins, Yen & Chou, 2000)

The next section looks at the different types of disasters. Many companies omit some disasters from the BCP based on their geographical location, environment and so on.

2.4 Disaster Events

To be able to beat your enemy is to understand or know your enemy. This section deals with what is a disaster and the elements that makes up a disaster.

A disaster as an event that is likely to cause significant disruption in an organization's operations for a period of time (Snoyer and Fischer, 1993).

IT Disasters are: (Semer, 1998)

- Natural disasters, such as fires, earthquakes, lightning, storms, and static electricity;
- Software malfunctions;
- Hardware or system malfunctions;
- Power outages;
- Computer viruses;
- Man-made threats, such as vandalism, hackers, and sabotage;
- Human error, such as improper computer shutdown, spilling liquids on the computer, and vandalism

No longer is nature's fury the only thing we fear, technological disasters, riots and human carnage over the years have played an equal if not larger share in disasters (Sayen, 2008).

Five different scenarios for IT catastrophic disasters where BCP becomes a necessity: (Pit & Goyal, 2004)

- Loss of building
- Loss of key personnel
- Loss of proprietary information
- Loss of telephone systems
- Loss of corporate stations

Disasters, regardless of cause, are characterized by a sudden and, for the most part, unexpected occurrence that demands timely actions to alleviate the situation (WMA, 2010).

During the period when the organization relies on the new system, it runs a greater risk of disaster, perhaps a greater one than when using the old system. This is because, on top of the likely causes of system disaster, there are also risks that stem from the fact that the system is new, such as (Aggelinos & Katsikas, 2011):

1. The system functions are not stabilised (both with respect to software and hardware)
2. Frequent alterations-corrections are made to the system, hence concrete, final documentation is missing.
3. A large number of security objects have not been completely checked or have not been implemented.
4. Staff are not completely familiarised with the system administration nor with the available troubleshooting options.

There are many potential disruptive events and the impact and probability level must be assessed to give a sound basis for progress. To assist with this process the following list of potential events has been produced (Clifton, 2000):

- Environmental Disasters
  - Tornado
  - Hurricane
  - Flood
  - Drought
  - Earthquake

  - Electrical storms
  - Fire
  - Subsidence and Landslides
  - Freezing Conditions
  - Contamination and Environmental Hazards
  - Epidemic
- Organized and/or Deliberate Disruption
  - Act of terrorism o Act of Sabotage
  - Act of war
  - Theft
  - Arson
  - Labour Disputes / Industrial Action
- Loss of Utilities and Services
  - Electrical power failure
  - Loss of gas supply
  - Loss of water supply
  - Petroleum and oil shortage
  - Communications services breakdown
  - Loss of drainage/waste removal

A crisis or disaster can be any emergency that happens suddenly, that disrupts the routine of the organization. All of the above-mentioned disaster events should be taken into account when developing a BCP to mitigate the recovery risk (Phelps, 1986).

2.5 Conclusion

In conclusion the ideal, complete, comprehensive plan, understood by all concerned, should be what all business recovery managers would no doubt like to achieve or aspire towards, that is being able to recover from a disaster with minimal downtime and the least amount of impact on the continuation of business (Maslen, 1996). Even though some of the BCP Processes as directed by Pitt & Goyal (2004), Chow (2000), Al-Zahrani (2009), Botha & Von Solms (2004) and (Wan (2009) covered most of the common processes and might be adequate for some business it clearly weren’t sufficient in preventing the

companies that were studied in this research in experiencing minimal downtime during their respective disasters.
Maslen, (1996) describes that in reality, any BCP has limitations, and will only be as good as the people who are involved with it. A BCP alone will not teach the team(s) to respond to and manage a crisis or disaster, but rather their commitment thereof.

We most commonly hear the term “failure to plan, is planning to fail”, therefore it is important that BCP cover all areas of business to ensure quick uptime with minimal losses and to provide staff with adequate training in the BCP process. It is so far evident from the above literature that certain criteria within the Business Continuity Plan need to be in place and even though all the research questions have been answered many companies still cannot answer why BCP often fails to help organisations avoid prolonged downtime after a disaster event. The literature presented some processes and considerations to be taken into account inside BCP processes such as obtaining management approval, performing a BIA, creating a BCP; testing and maintaining the BCP. Even though these processes are common, this study will show that additional process has been added after the research has been conducted.

In summary a BCP is a complex yet important document ensuring that a business recovers from a disaster effectively and quickly and that business disruptions are minimised and managed.

The table below summarises the various BCP Processes as shown in the literature, highlighting the Source, Author and Research Methodologies adopted for each.

Table 5: BCP Process based on source, research method and author

Process	Source	Research Method	Author
Seven-step contingency planning process	Contingency Planning Guide for Federal	Case study approach based on guidelines for	(Swanson, Lynes & Gallup, 2010)

	Information Systems Contingency Planning Guide for Federal Information Systems	Federal Organizations or Government Systems	
BCP Lifecycle (adopted from British Standards for BC www.bs25999.net)	Decision making assessment model throughout IT business continuity planning (BCP) lifecycle in small or medium-size organizations in Saudi Arabia	Qualitative and then a quantitative approach based on the answers derived from the qualitative research.	(Al-Zahrani, 2009)
Strategy developed by Aims and Methods	Business Continuity Psychology - From Strategy to Benefits?	Case Study approach researching an International Chemical Company	Gardener (2010
Standard Chartered Bank's BCP methodology (Heng, 1996)	Business continuity planning as a facilities management tool	Quantitative methodology	(Pitt & Goyal, 2004)
Risk reduction programme	A project planning process for business continuity	Case study approach based on real-life events	(Karakasidis, 1997)
Seven-phase BCP methodology	A cyclic approach to business continuity planning	Case study approach at a small organization	(Botha & Von Solms, 2004)
A Cyclic approach	A cyclic approach	Case study	(Botha & Von

to BCP	to business continuity planning	approach at a small organization	Solms, 2004)
“The Plan” that result from BCP	Business continuity planning	Case Study based on September 11 disasters.	(Savage, 2004)
5 Main steps in a BCP	Business continuity planning. It's a critical element of disaster preparedness. Can you afford to keep it off your radar?	Case Study based on September 11 disaster and other issues.	(Rozek & Groth, 2008)

As most of the research method for this type of study has been a based on case studies with qualitative approach, this research will also adopt the qualitative approach whereby the BCP Manager or Risk Manger of four companies based in the Western Cape will be interviewed by using open ended questionnaire to form four different case studies.

CHAPTER 3: CONCEPTUAL FRAMEWORK

A conceptual framework is a design of the primary sections of a system that shows interrelationships between one another and how they interact with each other (Bateman et al, 2011). Conceptual frameworks are developed to describe abstract occurrences that occur within similar circumstances (Rudestam and Newton, 1992) A conceptual framework is a structure of what has been learned to best explain the natural movement of an occurrence that is being studied (Camp, 2001).

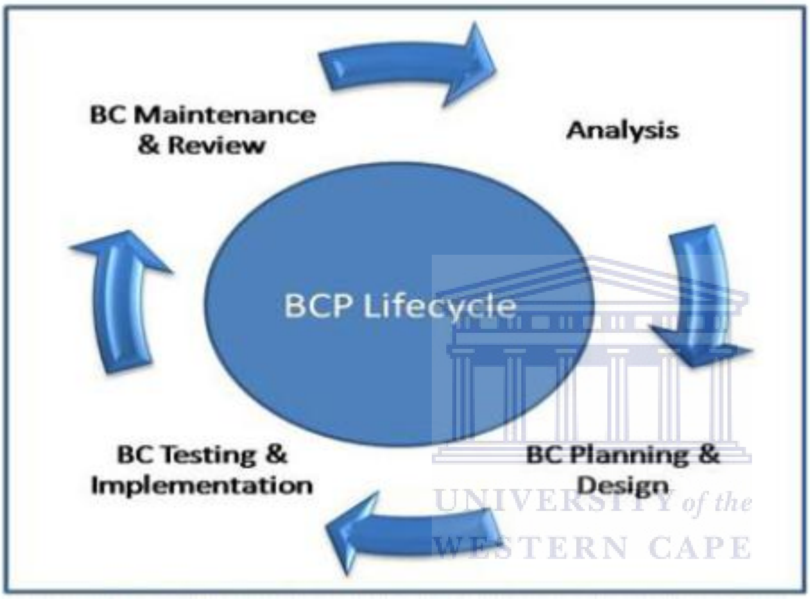

Figure 9: BCP Lifecycle (adopted from British Standards for BC)

Al Zahrani (2009) identified the above Figure as a common model of the BCP lifecycle. By using this model as well as on the most common concepts that were derived from various authors in the literature review section 2.1.4 indicated in Figure 8 as well as in Figure 10 below, this model was used to form the conceptual framework for this study. These common concepts are:

1. Management Approval: Organization management plays an important role in BCP development. Most of the potential decision makers are from management (Chow, 2000). Prior to starting a BCP it is important to obtain senior management approval and support (Pitt & Goyal, 2004). The board of directors or executive committee must be persuaded that BCP is important so that they can make the resources available (Savage, 2000).

2. Business Impact Analysis (BIA): During the BIA phase crucial business processes are recognized and then analysed (Botha & Von Solms, 2004). BIA is a process that identifies potential impacts on business in event of losing organizational resources (Al-Zahrani, 2009). The primary objective of the BIA is to gather data and review alternative courses of action. The gathering of the data allows management to decide which aspects are important to the business (Pitt & Goyal, 2004). The business impact analysis (BIA) is a critical part of planning for business continuity (Wan, 2009).
3. Develop an efficient and effective plan: This phase includes defining the scope and objectives of the plans, creating emergency procedures and the design of recovery solutions and procedures, as well as estimating costs and resources of developing the organization BCP (Pit & Goyal, 2004). It also involves documenting activities that are crucial to prepare an organization for possible disasters (Savage, 2000). A detailed functional plan must be developed for every process that was identified in the BIA phase (Botha & Von Solms, 2004).
4. Testing the plan: To establish an effective and efficient BCP it is imperative to implement regular testing exercises (Pit & Goyal, 2004). 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 key activities in this phase include testing and training of staff who are involved in the recovery process (Botha & Von Solms, 2004). After developing the plan it is just logical to test the plan at regular intervals ensuring that the plan remains current and can measure up to severe examinations (Savage, 2000)
5. Maintaining the plan: A number of plans will fail following the testing phase. It is critical that shortfalls be implemented back into the plan (Pit & Goyal, 2004). In other words regular review and development ensures that the plan is up to date (Botha & Von Solms, 2004). At times plans are constructed with passion and care, but are often left on the shelf and not updated regularly (Savage, 2000).

Based on the above it is important to note that each concept is dependent on the one that follows. For example you cannot maintain a plan if you did not test the plan, or you cannot test a plan if you don't have a plan.

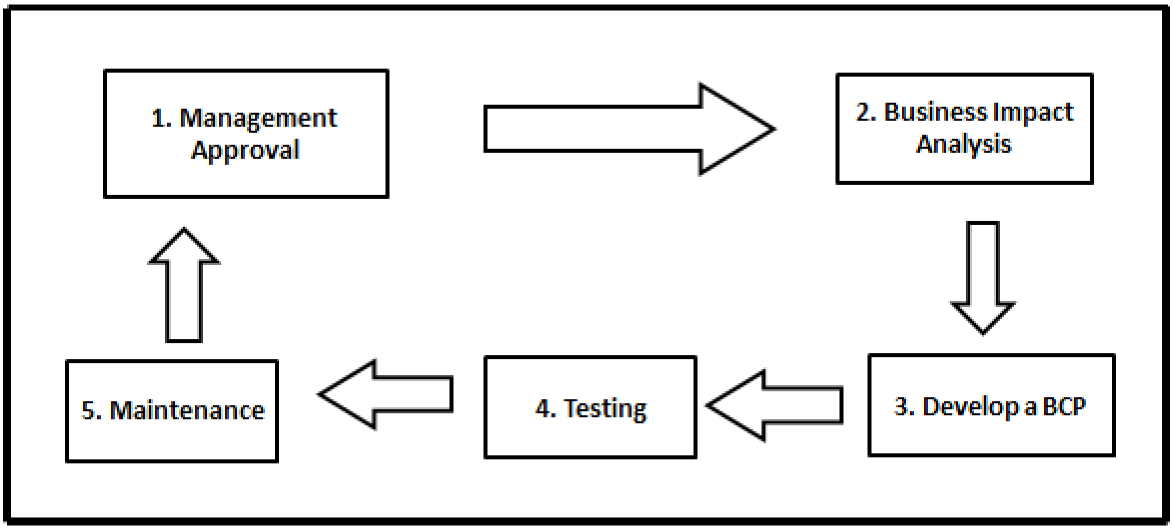

Figure 10: Conceptual Framework (Based on BCP common processes)

The aim of this study is to develop a new model using the conceptual framework model as depicted in figure 11 above as a base and then incorporating certain processes from Table 5 above to finalize the new model. This new model will include steps that will enhance the BCP of the companies that were interviewed thereby allowing them to reduce the recovery time after a disaster.

CHAPTER 4: RESEARCH METHODOLOGY

4.1 Introduction

This chapter describes the research design as well as outlining the research methodologies, the data collection method, the relevant data processing techniques and the method of interpreting the data collected. It aims at providing an overview of the method applied to conduct the research and collect the necessary data in order to answer the questions outlined in the research questionnaire.

The main objective of research is to find out the truth which is hidden and which has not been revealed as yet (Lastrucci, 2002). Lastrucci, (2002) is of the opinion that even though each research study has its own precise purpose, we may think of research objectives as falling into a number of broad groupings as follows:

1. To gain familiarity with an event or to achieve new insights into it (studies with this purpose in view are termed as trial or formulate research studies);
2. To show accurately the characteristics of a certain individual, situation or a group (studies with this object in view are known as descriptive research studies);
3. To determine the occurrence when something transpires or when it is associated with something else (studies with this object in view are known as diagnostic research studies);
4. To test a theory of a causal relationship between variables (such studies are known as hypothesis-testing research studies).

A research design is a blue-print or a thorough plan for how a research study is to be conducted (De Vos & Fouche, 1998). According to Merriam (1991) a research design is similar to an architecture blueprint and can be described as a plan for collecting, organising and integrating information (data), which results in a specific end product (research findings). The selection of a design is determined by how the problem is shaped, the questions it raises and by the type of end product desired.

Research is usually derived from some need or in order to have some purpose (Bless & Higson-Smith, 1995). Natural sciences research, at the one spectrum, is determined by the needs of production, commerce and industry, while social sciences research, at the other, is rooted in the need for enquiry about general management and control of social affairs (Bless & Higson-Smith, 1995). Research is undertaken broadly to (Singleton, 1993):

1. Explore a phenomenon,
2. describe a specific community and
3. examine and formally test relationships among variables.

Research in Information systems provides a rich scope of enquiry because of its multi-disciplinary and trans-disciplinary nature (Pather & Remenyi, 2005). This is because personal and social constructs have significant an impact on the way technology is used, and which explains the qualitative approach of this study (Mercer, 2001). This study proceeded along an interpretative pathway in the analysis of its data.

The methodological dimension of research is distinguished on three levels, namely methodological paradigms, research methods and research techniques (Mouton, 1997). The methodological paradigm is the most abstract level, which includes the distinction between qualitative, quantitative and participatory research. Research methods are those that are used in certain stages of the research process, for example sampling, data collection and data analysis. The three levels are demonstrated in Figure 11 below.

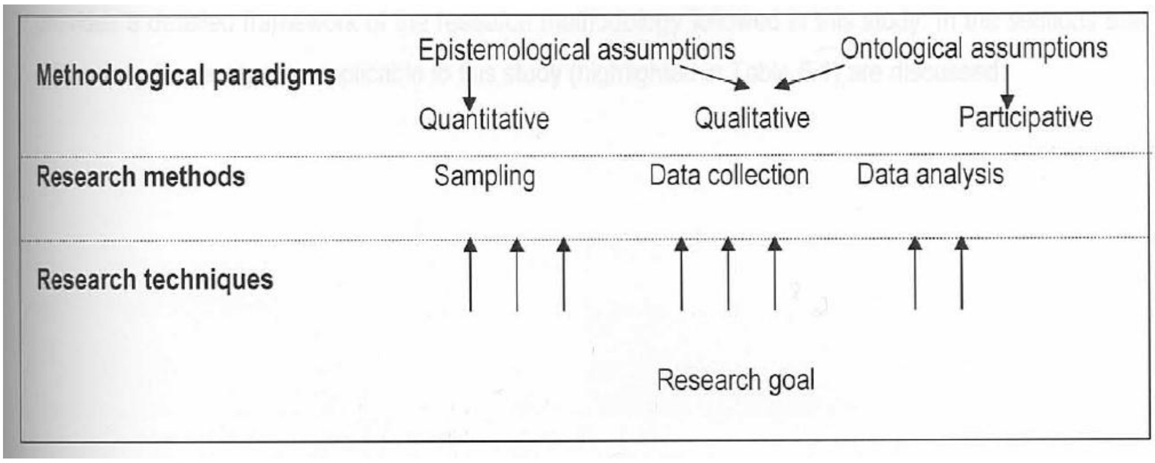

Figure 11: Levels in methodological dimension (Mouton, 1996)

There are two basic approaches to research, namely, a quantitative approach and the qualitative approach (Lastrucci, 2002). According to Hancock (2002) the collection of information for research purposes are divided into two approaches: quantitative research and qualitative research.

4.2 The quantitative research method

Research which originates in the natural sciences such as biology, chemistry, physics, geology etc. is focussed on investigations which are observable and measurable in some way. Such observations and measurements can be made objectively and repeated by other researchers. This process is referred to as "quantitative" research (Hancock, 2002).

Collis and Hussey (2003) are of the opinion that quantitative research is more concerned with questions about

- How much?
- How many?
- How often?
- To what extent?

Quantitative research is 'Explaining phenomena by collecting numerical data that are analysed using mathematically based methods (in particular statistics)' (Aliaga & Gunderson, 2002).

Quantitative research is a formal, objective, systematic process in which numerical data is used to obtain information about the world. This research method is used:

- to describe variables;
- to examine relationships among variables;
- to determine cause-and-effect interactions between variables (Burns & Grove 2005)

Quantitative research is therefore conclusive in its purpose as it tries to quantify the problem and understand how prevalent it is by looking for projectable results to a larger population. Here we collect data through surveys (online, phone, paper), audits, points of purchase (purchase transactions), and click-streams.

4.3 The qualitative research method

Qualitative research involves the collection, analysis and interpretation of data that is not easily reduced to numbers (Murphy, 2007). Research which attempts to increase our understanding of why things are the way they are and why people act the ways they do is “qualitative” in nature (Hancock, 2002). Hancock, (2002) is of the opinion that qualitative research would answer the following questions:

- Why people behave the way they do
- How opinions and attitudes are formed
- How people are affected by the events that go on around them
- How and why cultures have developed in the way they have
- The differences between social groups

Qualitative methods produce information only on the particular cases studied, and any more general conclusions are only hypotheses. Therefore qualitative methods can be used to verify, which of such hypotheses are true.

The goal of understanding a phenomenon from the point of view of the participants and its particular social and institutional context is largely lost when textual data is quantified (Kaplan and Maxwell, 1994).

In qualitative research, four types of problems can occur as a result of poor procedures (Erickson, 1986). These include:

1. inadequate amounts of evidence,
2. inadequate varieties of kinds of evidence,
3. inadequate attention to disconfirming evidence and,
4. The lack of attention to discretion.

Bearing this in mind, this study was designed to be explicitly descriptive and pragmatic, with no claim to generalise or externalise the findings but to build upon limited research and form a unique interpretation of events (Creswell, 1994).

A qualitative approach best suits this type of research since understanding social data is not necessarily best arrived at using numerical and statistical methods (Pather & Remenyi, 2005). Qualitative researchers are those interested in how people make sense of the world and how they experience events and try to understand specific conditions and how people manage these conditions (Priest, 2010).

IS research has generally shifted away from technological to managerial and organisational issues, with an increased interest in qualitative research methods (Myers, 2004). Qualitative study is as an inquiry process of understanding a social or human problem, based on a complex, holistic picture, formed with words, and reported in a natural setting (Marzanah, 2009). Qualitative research consists of a set of interpretive, material practices that make the world visible and turn it into a series of representations, including field notes, interviews, conversations, photographs, recordings, and memos to the self (Kohlbacher, 2005). Kohlbacher (2005) also states that qualitative researchers study things in the natural settings, attempting to make sense of, or to interpret, phenomena in terms of the meanings people bring to them. Qualitative research is a means of exploring an area of human experience, in order to understand how humans make sense of their world. It allows us to identify and describe topics or phenomena about which little is known, and explore and explain the scope and meaning of such phenomena (Priest, 2010).

Based on the above a qualitative research methodology was utilized for this study in order to capture the opinions of the participants which are key to this study.

4.4 Qualitative research designs

According to Myers (2009) there are four research methods:

1. **Action research**: Action research has been accepted as a valid research method in applied fields such as organization development and education. Action research aims to contribute both to the practical concerns of people in an immediate problematic situation and to the goals of social science by joint collaboration within a mutually acceptable ethical framework (Rapoport, 1970).
2. **Ethnography** is a qualitative research method that is used by anthropologists to describe a culture. Cultures usually consist of origins, values, roles, and material items associated with a particular group of people. Ethnographic research attempts to describe a variety of aspects and norms of a cultural group to enhance understanding of the people being studied (Byrne 2001).

3. **Grounded theory** is a qualitative research approach that was originally developed by Glaser and Strauss in the 1960s. According to Hancock (2002) this methodology originated with Glaser and Strauss and their work on the interactions between health care professionals and dying patients. The main feature is the development of new theory through the collection and analysis of data about a phenomenon.
4. **Case study research**: Although there are numerous definitions, Yin (2003) defines the scope of a case study as an empirical inquiry that investigates a current situation within its real-life context, especially when the boundaries between situation and context are not clearly evident. According to Hancock (2002) case studies can identify how a complex set of circumstances can come together to produce a particular manifestation. It is a highly flexible research method that employs any or all methods of data collection from testing to interviewing.

   A case study is considered by Benbasat (1987) to be viable for three reasons:

   - to study the occurrence in its natural setting;
   - to ask "how" and "why" questions, in order to understand the nature and complexity of the processes taking place;
   - to conduct research in an area where few, if any, previous studies have been undertaken.

Multiple cases are preferable when the purpose of the research is to describe occurrences and to develop and test theories. Multiple cases also permit cross-case analysis, a necessary feature for widespread generalisation of theories.
According to Yin (1994) case study research excels at bringing us to an understanding of a complex issue or object and can extend experience or add strength to what is already known through previous research.

The primary advantage of a case study is that it provides much more detailed information than what is available through other methods, such as surveys. Case studies also allow data to be collected from multiple methods (i.e., surveys, interviews, document review, and observation) to provide the complete story (Neale, Thapa & Boyce (2006)).

What gives case study its unique virtue is the depth or richness, completeness and wholeness in the processes of analysis, providing better understanding of complex social phenomena (Gerring, 2003).

The idiographic case study approach allows for a small sample that can range from a single, but preferably three participants, as long as the study is in-depth and represents the interpretive meanings of the participant's lived experience (Smith, Flowers & Larkin, 2009)

Since this study is based on actual events and scenarios, the case study research methodology was used as a means of collecting data from four companies around the Western Cape.

4.5 The Case Study as research choice

The selection of the research methodology depends on: the type of research questions asked; the extent of control that a researcher has over actual behavioural events and the degree of focus on present day as opposed to historical events (Yin, 1994). This research has adopted a case study approach as it is extensively used for information technology research (Lee, 1989). The Case Study research was the preferred strategy when "why", "what" and "how" questions which were asked. The focus of this study is to understand why companies that have BCP in place and perform regular testing, still experience prolonged downtime during a disaster. Case study is valuable in answering who, why and how questions in management research are applied to understand complex social phenomena because it allows the researcher to study real-life events while retaining their holistic and meaningful characteristics (Yin, 2003). Babbie & Mouton (2002) define a case study as the intensive investigation of a single unit that may include the examination of multiple variables and make mention of six types of case studies:

- Individual/single case study

- Community case study
- Social group study
- Studies of organizations and institutions
- Studies of events, roles and relationships
- Studies of countries and nations

There are different strategies which require diverse application depending on the situation being studied for example:

- For experiments, the form of questions are more 'How' and 'Why'
- For surveys, the form of questions are 'Who, What, Where, How Many, How Much'
- For Archival Analysis, the form of questions are 'Who, What, Where, How Many, How, Much'
- For Historical Analysis, the form of questions are 'How, Why'
- For Case Studies the form of questions are 'Why, What, How' (Yin, 2003).

Table 6 below illustrates the different strategies and the relevant situations for each strategy (Yin, 2003).

Table 6: Different Strategies (Yin, 2003)

Strategy	**Form of Research Questions**	**Requires Control of Behavioural Events**	**Focuses on Contemporary Events**
Experiment	How, why?	Yes	Yes
Survey	Who, what, where, how many, how much?	No	Yes
Archival analysis	Who, what, where, how many, how much?	No	Yes / No

History	How, why?	No	No
Case Study	Why, what, how?	No	Yes

The case study approach is used extensively for information technology research both as a research and a teaching tool (Alavi & Carson, 1992).

The case-study approach as part of a carefully designed research project that includes the following sections (Yin, 1994):

- an overview of the project (project objectives and case study issues)
- field procedures (credentials and access to sites)
- questions (specific questions that the investigator must keep in mind during data collection)
- a guide for the report (outline or format for the narrative)

A case study action process or roadmap should include determining the object of study (Patton, 2003):

- the object of study identified for this case was to create a new model to reduce downtime in the event of a disaster
- Selecting the case: the researcher strategically identified the case that suited the object of study as to determine why companies experience prolonged downtime during a disaster event
- Building initial theory through a literature review: the literature assisted framing the case study and establishing the validity and reliability of the findings
- Collecting and organizing the data gathering: appropriate instruments and protocols were established that focussed on the object of the study in order to avoid overwhelming amounts of data
- Analysing the data and reaching conclusions: The ultimate goal of case study is to, after having established the context, proceed with data analysis to uncover patterns, establish meanings, formulate conclusions and building a new model by adding to the most common BCP Processes.

A number of aspects must be considered when conducting case studies (Welman, 1999):

- The case must be studied within specified parameters;
- Irrespective of the data collecting techniques used, the purpose of case studies is not to describe what is observed, but to inductively identify recurring patterns and consistent regularities;
- Triangulation is frequently used in discerning such patterns e.g. (tape recordings, semi-structured interviews, newspaper reports, documentation, archival records and physical artefacts, are used to corroborate findings of a research project).

Case studies have both strengths and weaknesses. Table 7 below by Marzanah (2009) illustrates the strengths and weaknesses one has to be aware of when using the of case study method:

Table 7: Case Study methodology: Strengths and Weaknesses

Strengths	Weaknesses
1 Excels in understanding complex issue or object and can extend experience or add strength to what is already known through previous research	1 lack of control variables
2 Captures the local situation in greater detail and with respect to more variables than is possible	2 different interpretations by different people
3 Applicable to real life, contemporary, human situations and is accessible to the public in the form of written reports	3 Might contain unintentional biases and omissions in the description due to intense exposure to the study
	4 Study of a small number of cases can offer no grounds for establishing reliability or generality of findings

	5 Case study research as useful only as an exploratory tool

There are several methods for collecting data for a case study. The format and pattern of the study determine the nature of the data collection methods and how these are executed.

This section is to inform the reader of the various qualitative methods and the meaning of the terms. Since the object of this study is primarily to investigate the reasons for BCP failure in the event of a disaster and the ability of the BCP to restore business critical Information Systems to minimise operational disruption Benbasat et al. 1987).

4.6 Qualitative Data Collection Method

Qualitative research typically involves obtaining data through methods such interviews, on-site observations, and focus groups that in narrative rather than numerical form (Wyckoff 2007).

According to Hancock (2002) the three main methods of collecting data are:

- Individual interviews, which is the process of collecting information from individuals in three different ways:
  - Through structured interviews in which asking each respondent is asked the same question in the same way. This is mainly for quantitative research methods,
  - Through semi-structured interviews which consists of a series of open ended questions based on the topic. This would be mainly for qualitative research methods.
  - Unstructured interviews in which the interviewer has a limited number of topics, which are discussed in great depth. This would also be part of qualitative research methods.
- Focused groups are the process of collecting information from a group of people rather than individuals.
- Observations can be used when data collected through other means can be of limited value. Sometimes facial expressions and body

language are also “read” both by the interviewee as well as the interviewer.

Questionnaires are a good way of collating data and information swiftly (Bell, 1993). The aim of the questionnaire was to:

- ascertain whether the solutions suggested by the literature would be beneficial
- collate the data and find commonalities
- keep the interview process consistent and effective

Qualitative data collection utilizes rich and diverse data to answer questions and variability and complexity of human life. Table 8 below illustrates six different sources of evidences Yin (2003).

Table 8: Data Collection Methods (Yin, 2003)

Source	**Method**	**Comments**
Documents	Communiqués and written reports Administration documents Formal studies or evaluations Newspaper and articles from the mass media	This kind of information is likely to be relevant to every case study topic
Archival records	Service records Organisational records Maps, charts and lists Survey data and personal records	Often in computerised form
Interviews	Open-ended nature Focused Survey	The most important and essential source of case study information

Direct observation	Formal data Casual data	
Participant-observation	Being resident in a neighbourhood Functional roles in a environment Staff member in an organisational setting Being a key decision maker	Special mode of observation where the investigator is not a passive observer
Physical artefacts	Technological device Tool or instrument A work of art Other physical evidence	Less relevant potential in most typical kind of case study

A questionnaire is a series of written questions on a topic about which the subjects' opinions are sought (Sommer & Sommer, 2001). Questionnaires can be self-administered, that is

- When people answer a questionnaire they have received in the mail or at some event.
- When people are asked questions by an interviewer and people answer the questions openly.

The most difficult aspect about a questionnaire is its construction and the interpretation of the results.

Because there are many ways to ask questions, the questionnaire is very flexible. Questionnaires should be developed and tested carefully before being used on a large scale. There are three basic types of questionnaires (Dawson, 2002):

- Closed ended Questionnaires
    - Closed ended questions include all possible answers/prewritten response categories, and respondents are asked to choose among them.
    - For Example is multiple choice questions and scale questions.

    - Type of questions used to generate statistics in quantitative research.
    - As these follow a set format, and most responses can be entered easily into a computer for ease of analysis, greater numbers can be distributed.
- Open-ended Questionnaire
    - Open-ended questions allow respondents to answer in their own words.
    - Open-ended questionnaires do not contain boxes to tick but instead leave a blank section for the respondent to fill in.
    - Where closed ended questionnaires might be used to find out how many people use a service, open-ended questionnaires might be used to find out what people think about a service.
    - As there are no standard answers to open-ended questions, data analysis is more complex.
    - As opinions are being sought and not statistics, fewer questionnaires need to be distributed.
- Combination of both closed and open-ended questionnaires may allow one to find out how many people use a service and what they think of the service in the same form. Alternatively, a questionnaire begin with a series of closed – ended questions, with boxes to tick or scales to rank, and then finish with a section of open-ended questions or more detailed responses.

For this study an open-ended questionnaire was distributed to the Risk and BCP Managers of each of the four participating companies. The questionnaire, (See Appendix A – Research Questionnaire), was emailed to all the selected participants prior to the interview.

The basis and origin for the open-ended questionnaire is displayed in the table below.

Table 9: Questions, Basis and Origin

Questions	Basis for Question	Origin
1. Does the company have a written business continuity	To establish whether the company has a BCP in place, as this is a	Section 2.2

plan?	prerequisite for the company that is interviewed.	
2. Where is the company's BCP kept and who has access to this document?	How accessible is this document? Are employees allowed access it when necessary.	Section 2.4.2
3. Are there any exclusions to your BCP such as personnel, natural disasters, and why?	To determine whether every disaster or threat was considered	Section 2.3
4. Does the DRP form part of the BCP or is it a separate plan altogether?	To determine whether the DRP is part of the BCP or a separate plan altogether	Section 2.2
5. Does business continuity and disaster recovery readiness have the support of top management in your organization?	If top management does not support the plan, this might possibly be a reason for BCP failure	Section 2.2
6. What happens if key personnel are not available during a disaster?	To determine whether the company is solely dependent on key personnel or whether alternative options are available. The answer to this question will identify the level of risk	Section 2.4.2
7. Has your organization identified which vendors may need	To determine whether this part within the plan has been considered as this	Section 2.4.1

access to your facility after a disaster?	could also lead to prolonged downtime.	
8. How often is the BCP reviewed or updated?	This is one of the most important points to the success of a BCP.	Section 2.4.1
9. How are business critical applications identified?	This question is to determine how critical applications are identified.	Section 2.2
10. Who is responsible for identifying these applications?	This question is to determine whether decisions are only from an IT perspective or whether the business owner is involved as well.	Section 2.2
11. Was your disaster covered by your plan, if no, why?	This question is to determine whether any of these disasters were covered.	Section 2.1
12. Do you perform back-ups faithfully and include every server and hard disk?	If a critical server or application is omitted this too can contribute towards prolonged recovery time or cause inability to recover at all.	Section 2.2
13. How often do you perform a BCP test? When tested, what were the results?	A major cause of BCP failure is when tests aren't performed regularly enough or when the tests do not include new applications and servers.	Section 2.4.1
14. Do you have unscheduled BCP	Unscheduled tests will keep the company aware	Section 2.4.2

test? If tested, did you pass your test?	and alert at all times so that those involved are familiar with the drill	
15. Does the company BCP highlight what are acceptable downtimes after specific disasters?	This question is to establish whether the company had highlighted specific downtime based on specific disasters and whether the Risk manager feels that these times are acceptable.	Section 2.4.1
16. Do you feel that these times are attainable?	To determine whether the downtime placed within SLAs are acceptable and attainable	Section 2.1
17. What was the impact of the disaster on business?	To establish whether income was lost or what other impact business suffered due to the severity of the disaster.	Section 2.4.1

Personal face-to-face interviews were conducted and a semi-structured questionnaire to keep the interviewer and interviewee focused and aligned with the research questions and objectives. Each interview lasted 30 to 40 minutes and was conducted at the premises of each of the companies. A digital recording device was used to record each interview. The Risk Manager or BCP Manager from each of the four companies within the Western Cape, who each had BCP in place, but still experienced prolonged downtime during a disaster were interviewed.

In conclusion, this chapter has formed an integral part of this study and described the research strategy, design, methods and techniques used to obtain the final results.

CHAPTER 5: DATA ANALYSIS AND FINDINGS

This chapter will display the outcome of the interview analysis and discuss the findings as well as the case study of each company's disaster which led to this research. The purpose of the interviews was to determine why companies experienced prolonged downtime during a disaster event. The data collected was analysed based on all interviewee responses which is also available on digital recording.

5.1 Data Analysis

According to Hancock (2002) data analysis is the process of summarizing and presenting all data collected in a way that presents the most important features. Hancock is also of the opinion that in qualitative research different techniques are used to discover the bigger picture such as

- Transcribing which is the process of writing down everything while conducting the interview or that was recorded during the interview.
- Content analysis which refers to the process of interpreting the data collected.
- Tape analysis which entails the process of replaying the recorded interview to analyze the data rather than transcribing.

Seidel (1998) is of the opinion that analysing qualitative data is a simple process that consists of three simple steps as shown in Figure: 12

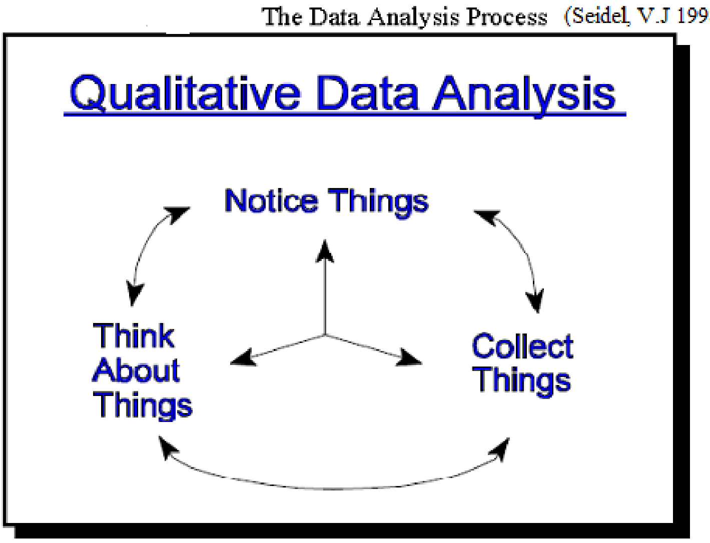
The Data Analysis Process (Seidel, V.J 1998)
Qualitative Data Analysis
Notice Things
Think About Things
Collect Things

Figure 12: The Data Analysis Process

1. Noticing things means making observations, writing field notes, tape recording interviews and gathering documents in order to produce a record of things that you have noticed.
2. Collecting things is similar to putting the pieces of a jig-saw puzzle together. After noticing and naming the data, the next step is to sort the data to determine what would be useful to the research study.
3. Thinking about things is the process of examining the things you have collected. Your goals are to make sense out of each collection, look for patterns and relationships both within a collection, and also across collections and make general discoveries about the phenomena being researched.

Processing and analysing data involves a number of closely related operations which are performed with the purpose of summarizing the collected data and organizing these in such a manner so as to answer the research questions (Dawson, 2002). The Data Processing operations are:

1. Editing- a process of examining the collected raw data to detect errors and omissions and to correct these when possible.
2. Classification- a process of arranging data in groups or classes on the basis of common characteristics, depending on the nature of phenomenon involved

   2.1 Classification according to attributes: here data is analysed on the basis of common characteristics which can either be:

   2.1.1 Descriptive such as literacy, sex, religion and so on

   2.1.2 Numerical such as weight, height, income etc.

The researcher must ensure that the data is converged in an attempt to understand the overall case, not the various parts of the case, or the contributing factors that influence the case (Baxter & Jack, 2010).

5.1.1 Data Analysis using a computer program

Qualitative researchers often find themselves overwhelmed by the amount of data and in need of tools to extend their human senses (Meyer & Avery, 2008). This has led the development of a number of software packages designed for this purpose. An often overlooked option is Microsoft Excel. Excel is generally considered a number cruncher. However its structure and data manipulation and display features can be utilized for qualitative analysis.

Microsoft Excel was used as a data analysis tool for this study. Responses for each company were entered into an Excel spreadsheet, next to each question from the open-ended questionnaire. In this way the response for each company was displayed on a separate Excel spreadsheet. Data was analyzed by entering the responses of each respondent and creating columns marked Company A to Company D representing each of the four companies that participated in the research as illustrated in Appendix B. Common answers were grouped together for each company.

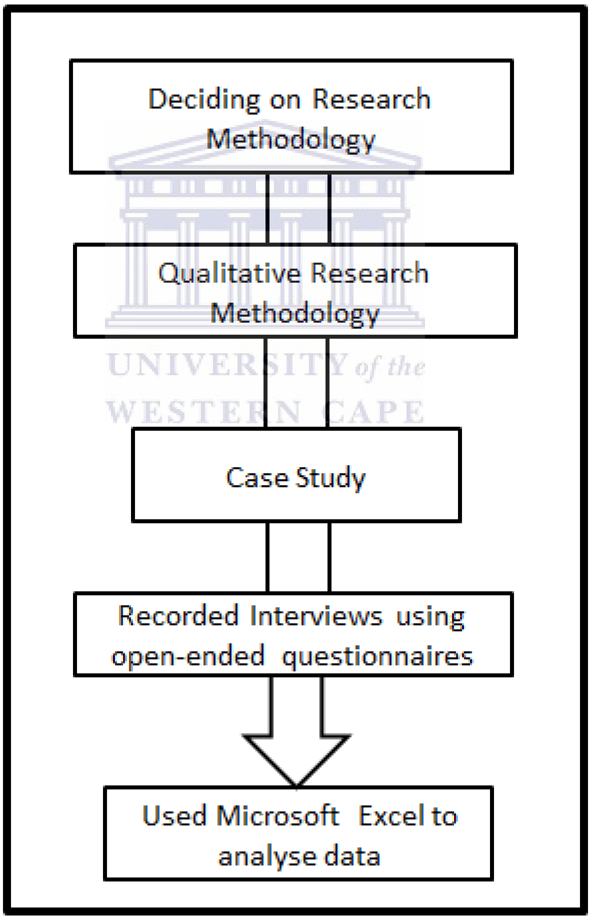
Deciding on Research Methodology
Qualitative Research Methodology
Case Study
Recorded Interviews using open-ended questionnaires
Used Microsoft Excel to analyse data

Figure 13: Research Process

The above process (Figure 13) was used to obtain the objective of this study which is why do companies that have BCP in place still experience prolonged downtime during a disaster. The above process was followed for each of the four companies so that the original focus which is why do companies that have BCP in place and perform regular testing still experience prolonged downtime during a disaster is maintained. The findings attained through the research process are presented in this chapter

Before embarking on the research project a Non-Disclosure Agreement (NDA) with each company that was interviewed had to be signed. It was agreed that none of the companies or their employees would be mentioned in this research paper.
The Risk Manager or BCP Manager from each of the four companies that are based in the Western Cape was interviewed. Each of the companies has BCP in place, test it regularly but still experience prolonged downtimes during a disaster.

5.2 Findings - Case Studies

In order to protect the companies and participants, they will be referred to as Company A to D. Their stories are as follows:

5.2.1 Finding of Case Study 1 (Company A)

5.2.1.1 Introduction to Company A

Company A is one of South Africa's largest outdoor retail stores, with more than one hundred branches all over South Africa as well as in Namibia and Botswana. They are considered a well-established and reputable retail outlet in South Africa's retail market. The company employs about 1000 to 1500 permanent and casual staff nationally. About 500 of these permanent employees stationed at the Head Office alone. Each branch is equipped with the latest computer terminals on which the Point of Sale (POS) software is installed. These computer terminals connect to a computer known as the back office terminal which is situated in the store manager's office. The back office terminal for each store constantly communicates with the servers at Head Office to report back sales transactions, stock levels of each item, credit card transactions and so on. If a server "goes down" meaning that either the server crashed or the network lines between a store and the Head Office are not operational, that store is "shut out" electronically to the outside world and has to trade manually. This means that staff members within the store have to write down each cash transactions in an invoice book. No debit or credit card transactions are allowed, and in today's age that is an imperative part of every business as most patrons use their debit or credit cards.

5.2.1.2 Disaster of Company A

On the 20th of September 2011 the company's Head Office in Cape Town experienced a power failure. Although the Datacentre is equipped with an Uninterrupted Power Supply (UPS), it only lasted for 10 minutes which was just enough time to allow the system administrator to shut-down all servers. All 220 VAC power equipment such as servers, network switches, routers and other electronic equipment were now non-operational. Communication between all stores and Head Office was down, thereby causing stores to be electronically "shut out", thus causing sales staff within the stores to write down each cash transactions in an invoice book as no debit or credit card transactions could be processed.

The impact of the disaster on business was as follows:

- All stores had to trade manually and turn away customers that wanted to purchase items using a debit or credit card.
- No bookings or reserving of items for customers were available.
- Checking for a particular item at a different branch for customers was not possible.
- Most of the staff at Head Office was unable to perform their duties until the power was restored as everyone relied on various systems to perform daily tasks.
- The power failure lasted for 4 hours, which is an extremely long time for any retail company.

After interviewing the Risk Manager it was established that the company overlooked the fact that they would ever experience a power failure seeing that the company is on the same power substation as parliament. The company had therefore made no provisions or alternatives for the event of a power failure.

This decision had proved to be catastrophic. As previously stated a disaster of this magnitude can definitely cause both financial and reputability damage.

The table below provides a summary of the questions answered by the Risk Manager.

Table 10: Summary of answers (Company A)

Questions	Answers
1. Does the company have a written business continuity plan?	Yes
2. Where is it kept and who has access to this document?	Kept on SharePoint for the whole company to view, as well as in the IT department and at the DR Site
3. Are there any exclusions to your BCP such as personnel, natural disasters, and why?	Yes, lack of additional personnel. We have exclude events such as floods, tornadoes and so on. Non critical business applications due to budget constraints. Power failures as company is on the same sub-station as parliament and the chances that parliament would experience a power failure is very slim. Not sufficient business and technical staff involve in the plan
4. Does the DRP form part of the BCP or is it a separate plan altogether?	The DRP is part of the BCP
5. Does business continuity and disaster recovery readiness have support of top management in your organization, if no why?	Yes, There is a committee that monitors all the BCP tests. Top management does not fully understand the importance of BCP
6. What happens if key personnel are not available during a disaster?	Our BCP and DR is managed by a third party who has the necessary resources to assist when key personnel is not

	available
7. Have your organization identified which vendors may need access to your facility after a disaster?	Yes only for specific vendors
8. How often is the BCP reviewed and updated?	We do our testing every 6 months and generally this is when we update our plan, as we test our application changes in the test as well.
9. How is business critical applications identified?	Through general consciences among IT and Business. No specific Business Impact Analysis Tools
10. Who is responsible for identifying these applications?	IT and Business
11. Was your disaster covered by your plan, if no why?	**No, our company shares the same sub-station as parliament and the chances that parliament would experience a power failure is very slim. This factor was taken for granted.**
12. Do you perform back-ups faithfully and include every server and hard disk?	No, budget constraints due to the size of data that will be saved to disk. Disks are expensive. Test servers. Non critical business applications. All business critical servers are backed up on a daily basis.
13. How often do you perform a BCP test? If tested, did you pass your test?	Every 6 months. No not all the time, but then again that it the purpose of a BCP test to identify our shortcomings.
14. Do you have unscheduled BCP test? If yes, did you pass your test? If no, why?	No, too expensive. Testers need to be arranged before the time.
15. Does the company BCP highlight what are acceptable downtimes?	It was agreed by auditing committee that there is a recovery window for BC

	purposes.
16. Do you feel that these times are attainable?	Yes, we are currently comfortable with the time allocated.
17. What was the impact of the disaster on business?	SLA was missed with business. Retail outlet had to trade manually as databases resides at head office. No stock updates were sent to and fro from retail outlet. Only cash transactions.

The answer to question 11 in Table 10 above is an indication that the company took the power factor for granted, even though in Section 2.4 in the Literature review chapter, where Semer (1998) defines that power failures are one of the most common disaster that a company can experience.

Questions 2, 5, 6, 8, 9, 13 & 15 in the above table are specifically linked to the key elements of an effective BCP as depicted in Section 2.1.3 of the literature review chapter. The purpose for these questions was to determine whether Company A had applied the key elements of a BCP.

Table 11 below is an analysis of the answers to the questions that relates to the key elements of an effective BCP as per Section 2.1.3 of the Literature Review Chapter.

Table 11: Analysis of Company A's responses to research question linking to BCP Elements

Questions	**Responses**	**Comply with key elements of an effective BCP as per Section 2.1.3**
2. Where is the company's BCP kept and who has access to this document?	Kept on SharePoint for the whole company to view, as well as in the IT department and at the DR Site	Before a plan can be tested, employers and employees need to be familiar with the content of the plan and their role in the response and recovery. This can be done by reading through the plan

		together and discussing how you would apply it to a fictional scenario.
5. Does business continuity and disaster recovery readiness have support of top management in your organization?	Yes, There is a committee that monitors all the BCP tests. Top management does not fully understand the importance of BCP	Get senior management involved and keep them committed.
6. What happens if key personnel are not available during a disaster?	Our BCP and DR is managed by a third party who has the necessary resources to assist when key personnel is not available	In order for a plan to succeed, there must be multiple agency cooperation and involvement.
8. How often is the BCP reviewed and updated?	We do our testing every 6 months and generally this is when we update our plan, as we test our application changes in the test as well.	Keep the plan current – Update the plan as applications gets updated
9. How are business critical applications identified?	Through general consciences among IT and Business. No specific Business Impact Analysis Tools	Identify critical businesses and supporting functions and perform business impact analyses.
13. How often do you perform a BCP test? When tested, what were the results?	Every 6 months. No not all the time, but then again that it the purpose of a BCP test to identify our shortcomings.	Test the business recovery process and evaluate test results
15. Does the company BCP highlight what are	It was agreed by auditing committee that there is a	Identify your recovery point objective (RPO) and

acceptable downtimes?	recovery window for BC purposes.	recovery time objective (RTO), making sure your data protection solutions can meet these requirements.

The answers to questions 2, 5, 6, 8, 9, 13 & 15 in Table 11 above is an indication that Company A conformed to some of the key elements of an effective BCP.

5.2.2 Findings of Case Study 2 (Company B)

5.2.2.1 Introduction to Company B

This company provides multi-jurisdictional legal, tax, fiduciary, investment and fund administration services to private, corporate and institutional clients. They provide the highest levels of expertise and competence and work in a way that is uniquely personal, proactive and responsive. The firm currently employs over 550 employees with 12 offices across Europe, the Caribbean and South Africa. It has over $125 billion worth of international assets under its administration. They have a deep understanding of multiple jurisdictions and industries, which has earned them various international accolades and the loyalty of their clients, many of whom have been with them for decades. Their private clients are families and individuals, entrepreneurs and senior business executives, whereas their corporate clients comprise of blue-chip corporations, listed and non-listed entities and multi-nationals and their institutional clients are fund managers from large, medium and small companies.

Being a financial institution requires that the company offer support 24/7 throughout the year to all its clients. The firm also acts as an outsourced company to various financial houses by administering all the clients' financial profiles. The SLA between the firm and these financial houses are that:

- There will be 100% uptime, allowing the financial houses to update the records of new and existing clients.
- Clients have 24 hours 7 days a week access to their investments and financial information.

- Clients of the financial houses are allowed to change or alter their investment profiles at any given time.

These SLA's are the core business of the company and the company thrive on its reputable and committed reputation to gain market share within this industry.

5.2.2.2 Disaster of Company B

The company has a web portal that allows all clients to check the status of their investments and also allows them to change their portfolio based on market reactions. The web portal is connected to a primary router that links into the Multiprotocol Label Switching (MPLS) and a secondary router that links to their disaster recovery site. The primary router connects the entire company both locally and internationally to its different divisions and to its clients. If for some reason this primary link fails there should be an automatic fail over the secondary link without any down-time or impact on business. The primary link failed on 14th July 2011. After an hour of investigating the network administrator discovered that the fail over to the secondary link did not occur automatically. He then manually switched over to the secondary link, only to discover that the router is not configured correctly and that no one within the IT department knows the correct configuration, as that router is the responsibility of an Internet Service Provider (ISP) company. The race was between the ISP and the network administrator to get either of the routers up. It took the network administrator four hours to reconfigure the primary router, whilst the ISP was still battling with configuring the secondary router.

After interviewing the company's Security and Risk manager it was discovered that the routers were overlooked and was never included in the BCP test. The company focused mainly on the actual servers and software that resides within the servers and not on the peripherals around the servers.

Due to the fact that trading and pricing updates could not be done, the impact of the disaster had been mainly financial as SLA's were not met. The company's reputation also suffered some damage.

Table12 below is a summary of the answers of the Security and Risk manager for Company B

Table 12: Summary of answers (Company B)

Questions	Answers
1. Does the company have a written business continuity plan?	Yes
2. Where is it kept and who has access to this document?	Kept on SharePoint for the whole company to view. The complete IT department. At the Disaster Recovery Site.
3. Are there any exclusions to your BCP such as personnel, natural disasters, and why?	Yes, lack of additional personnel. Not sufficient business and technical staff involve in the plan.
4. Does the DRP form part of the BCP or is it a separate plan altogether?	The DRP consist within the BCP.
5. Does business continuity and disaster recovery readiness have support of top management in your organization, if no why?	Yes
6. What happens if key personnel are not available during a disaster?	Vendors are on standby to assist. Support from vendors. There is an agreement with third party vendors for technical support in the event of a disaster.
7. Have your organization identified which vendors may need access to your facility after a disaster?	Yes only for specific vendors.
8. How often is the BCP reviewed and updated?	Annually. Real time replication, that allows all new applications to be included automatically.
9. How is business critical applications identified?	By the use of a matrix. A Business Impact Analysis Tool is used to determine the impact of each application.

10. Who is responsible for identifying these applications?	Each business unit will sign off on their own application.
11. Was your disaster covered by your plan, if no why?	**No, there was no connectivity.**
12. Do you perform back-ups faithfully and include every server and hard disk?	No, test servers. Non critical business applications. All business critical servers are backed up on a daily basis. Real time replication.
13. How often do you perform a BCP test? If tested, did you pass your test?	Every 6 months. We do not pass all the time. Once a year an ICT test is performed. This is a technical test to ensure that we are able to restore all servers. A user test is done once a year to ensure that all applications restored are fully operational.
14. Do you have unscheduled BCP test? If yes, did you pass your test? If no, why?	No, Company is not ready for it. Yes would like to do unscheduled tests.
15. Does the company BCP highlight what are acceptable downtimes?	Yes, form part of the BIA.
16. Do you feel that these times are attainable?	Yes.
17. What was the impact of the disaster on business?	SLA was missed with business. Clients could not trade. Financial impact. Possibility of losing clients.

The answers to question 11 in Table 12 above highlight that Company B did not perform a proper analysis of all its equipment, thereby causing them to overlook a router which is pertinent to their daily operations.

Questions 2, 5, 6, 8, 9, 13 & 15 in the above table are specifically linked to the key elements of an effective BCP as depicted in Section 2.1.3 of the literature review chapter. The purpose for these questions was to determine whether Company B had applied the key elements of a BCP.

Table 13 below is an analysis of the answers to the questions that relates to the key elements of an effective BCP as shown in Section 2.1.3 of the Literature Review Chapter.

Table 13: Analysis of Company B's responses to research question linked to BCP Elements

Questions	Responses	Comply with key elements of an effective BCP as per Section 2.1.3
2. Where is the company's BCP kept and who has access to this document?	Kept on SharePoint for the whole company to view. The complete IT department. At the Disaster Recovery Site.	Before a plan can be tested, employers and employees need to be familiar with the content of the plan and their role in the response and recovery. This can be done by reading through the plan together and discussing how you would apply it to a fictional scenario.
5. Does business continuity and disaster recovery readiness have support of top management in your organization?	Yes	Get senior management involved and keep them committed.
6. What happens if key personnel are not available during a disaster?	Vendors are on standby to assist. Support from vendors. There is an agreement with third party vendors for technical	In order for a plan to succeed, there must be multiple agency cooperation and involvement.

	support in the event of a disaster.	
8. How often is the BCP reviewed and updated?	Annually. Real time replication, that allows all new applications to be included automatically.	Keep the plan current – Update the plan as applications gets updated
9. How are business critical applications identified?	By the use of a matrix. A Business Impact Analysis Tool is used to determine the impact of each application.	Identify critical businesses and supporting functions and perform business impact analyses.
13. How often do you perform a BCP test? When tested, what were the results?	Every 6 months. We do not pass all the time. Once a year an ICT test is performed. This is a technical test to ensure that we are able to restore all servers. A user test is done once a year to ensure that all applications restored are fully operational.	Test the business recovery process and evaluate test results
15. Does the company BCP highlight what are acceptable downtimes?	Yes, form part of the BIA.	Identify your recovery point objective (RPO) and recovery time objective (RTO), making sure your data protection solutions can meet these requirements.

The answers to questions 2, 5, 6, 8, 9, 13 and 15 in Table 13 above, highlighted that most of the key elements of a BCP had been adhered to by Company B.

5.2.3 Findings of Case Study 3 (Company C)

5.2.3.1 Introduction to Company C

Company C is an African mobile communications company providing voice, messaging, data and converged services to over 45 million customers. From their roots in South Africa, they have grown their operations to include networks in Tanzania, the Democratic Republic of Congo ('DRC'), Mozambique and Lesotho. They also provide carrier and business services to customers in over 70 countries.

This company is one of the world's largest mobile communications companies that is currently listed on the JSE. Even though their Head Office is based in Johannesburg the company's technical stronghold is in Cape Town.

On a daily basis the service desk in Cape Town receives numerous calls from old and new subscribers, distributors and vendors for information, product updates and information. It is therefore imperative that all systems have a 100% uptime, allowing users to access information whenever from wherever as well as permitting vendors and agents to signup new subscribers or upgrade available contracts. If the system goes down or users, vendors, agents and distributors aren't able to access the system, no information of a particular user is available and no new contracts can be activated or existing contracts upgraded. This could have disastrous repercussion on the reputation of the company and might cause them to loose market value meaning a loss in revenue.

5.2.3.2 Disaster of Company C

On Saturday the 25th of August 2012 applications across multiple system platforms in Cape Town sporadically stopped functioning. Every client accessing the company's portal could not access, read, update or cancel information as the system would intermittently block access to the database server. Each scenario is listed as part of the BCP strategy, thereby informing the operator in the service department what to do in the event something happens; this scenario however was not listed. The operator did what he thought was a logical approach by rebooting the system every time in the hope that the system would reset itself. The telephones at the service desk rang all day from frustrated vendors as most of their patrons would walk out of the store causing a loss in revenue. After half the day had passed, the service desk operator decided to escalate the matter. Immediately the system administrator, network administrator and database administrator rushed to the Cape Town office. Seeing that the problem was intermittent it made diagnosing very difficult for the technical team, but after nearly two hours of investigation it was discovered that one of the application services would automatically restart itself. The system administrator immediately put alerts in place that should any of the services fail an email be sent to the appropriate parties concerned.

The interview with the Risk Manager revealed that the monitoring of the application services had been overlooked, and therefore was not listed in the BCP strategy documents that are given to service desk operators.

Seeing that the system was down for eight hours nationally, distributors and vendors had to turn away new and existing customers as they could not access the main server. This certainly had a great financial impact on the company and also damaged its reputation.

Table 14 below is a summary of the answers given by the Risk Manager for Company C.

Table 14: Summary of answers (Company C)

Questions	Answers
1. Does the company have a written business continuity plan?	Yes
2. Where is it kept and who has access to this document?	Kept on SharePoint for the whole company to view.
3. Are there any exclusions to your BCP such as personnel, natural disasters, and why?	No, everything is covered.

4. Does the DRP form part of the BCP or is it a separate plan altogether?	The DRP is part of the BCP. The BCP covers all the natural disasters. The DRP within the BCP covers the technical aspects.
5. Does business continuity and disaster recovery readiness have support of top management in your organization, if no why?	Yes, there is a Business Continuity Management (BCM) team that looks after enterprise wide BCP.
6. What happens if key personnel are not available during a disaster?	Vendors are on standby to assist. Support from vendors. All key personnel have alternative numbers from a different service provider. All critical services have standby and escalation procedures in place.
7. Have your organization identified which vendors may need access to your facility after a disaster?	Yes only for specific vendors. Service Level Agreements (SLA) is in place with specific vendors.
8. How often is the BCP reviewed and updated?	Every 6 months. Real time replication, that allows all new applications to be included automatically. Some critical applications are reviewed quarterly.
9. How is business critical applications identified?	By the use of a matrix. All business critical services and systems are rated as per criticality. (Mission critical, business critical, non-critical).
10. Who is responsible for identifying these applications?	Business owner. BCM Team.
11. Was your disaster covered by your plan, if no why?	**No, We did not consider monitoring any services as we are already monitoring the software.**
12. Do you perform back-ups faithfully and include every server and hard disk?	No, test servers. Non critical business applications. All business critical servers are backed up on a daily basis. Real time

	replication.
13. How often do you perform a BCP test? If tested, did you pass your test?	Every 6 months. No we do not pass all the time. Some applications are tested quarterly. Insufficient disk space on server.
14. Do you have unscheduled BCP test? If yes, did you pass your test? If no, why?	No.
15. Does the company BCP highlight what are acceptable downtimes?	Yes, Uptime is 99%.
16. Do you feel that these times are attainable?	Yes, Time frames has been thoroughly tested and agreed upon. Due to the nature of our business we need to be up all the time.
17. What was the impact of the disaster on business?	Possibility of losing clients. Entire call centre was down. Reputation was damaged

The answer to question 11(in bold) in Table 14 above proved that not only should the software be monitored, but also the application as well as services of any application.

Questions 2, 5, 6, 8, 9, 13 & 15 in the above table are specifically linked to the key elements of an effective BCP as depicted in Section 2.1.3 of the literature review chapter. The purpose for these questions was to determine whether Company C had applied the key elements of a BCP.

Table 15 below is an analysis of the answers to the questions which relate to the key elements of an effective BCP as shown in Section 2.1.3 of the Literature Review Chapter.

Table 15: Analysis of Company C's responses to research question linking to BCP Elements

Questions	Responses	Comply with key elements of an effective BCP as per Section 2.7
2. Where is the company's BCP kept and who has access to this document?	Kept on SharePoint for the whole company to view.	Before a plan can be tested, employers and employees need to be familiar with the content of the plan and their role in the response and recovery. This can be done by reading through the plan together and discussing how you would apply it to a fictional scenario.
5. Does business continuity and disaster recovery readiness have support of top management in your organization?	Yes, there is a Business Continuity Management (BCM) team that looks after enterprise wide BCP.	Get senior management involved and keep them committed.
6. What happens if key personnel are not available during a disaster?	Vendors are on standby to assist. Support from vendors. All key personnel have alternative numbers from a different service provider. All critical services have standby and escalation procedures in place.	In order for a plan to succeed, there must be multiple agency cooperation and involvement.
8. How often is the BCP reviewed and updated?	Every 6 months. Real time replication, that allows all new applications to be included automatically. Some critical	Keep the plan current – Update the plan as applications gets updated

	applications are reviewed quarterly.	
9. How are business critical applications identified?	By the use of a matrix. All business critical services and systems are rated as per criticality. (Mission critical, business critical, non-critical).	Identify critical businesses and supporting functions and perform business impact analyses.
13. How often do you perform a BCP test? When tested, what were the results?	Every 6 months. No we do not pass all the time. Some applications are tested quarterly. Insufficient disk space on server.	Test the business recovery process and evaluate test results
15. Does the company BCP highlight what are acceptable downtimes?	Yes, Uptime is 99%.	Identify your recovery point objective (RPO) and recovery time objective (RTO), making sure your data protection solutions can meet these requirements.

The answers to questions 2, 5, 6, 8, 9, 13 and 15 in Table 15 above highlights that most of the key elements of a BCP had been adhere to by Company C.

5.2.4 Findings of Case Study 4 (Company D)

5.2.4.1 Introduction to Company D

Founded in 1997, Company D is a privately owned Internet Service Provider (ISP), providing broadband internet access and hosting solutions across South Africa to both home and business customers in equal measure.

With over 30 000 subscribers enjoying their world-class network experience, this company has consistently been independently rated as one of the leading ISPs in South Africa. In 2006 the company won their first title as Best ADSL

Service Provider in South Africa and this meant that they had to uphold there reputation by providing 24 hours a day, seven days a week internet access to users nationally.

There customers are supported by 120 staff members, who spend every day trying to go beyond the call of duty, which is why the company is close to achieving their goal of becoming South Africa's most loved and trusted ISP.

Some of their customers require support between Limpopo to London. It is therefore imperative that the internet lines and network connectivity be up and running at all times as businesses and individuals are dependent on them for Webhosting, Internet Services, emails and so on. Companies in this type of industry rely on their reputation to gain market share.

5.2.4.2 Disaster of Company D

On the16th of May 2012 the company lost network connectivity to the company that supplies them with bandwidth, and as a result all their clients could not connect to the internet. This meant that private as well as their business clients were unable to surf the net, check emails, perform online banking, download, whilst in addition businesses were not able to trade, communicate to their clients, and so on. The company battled the entire day with their supplier to get the line restored.

Even though their BCP covered all aspects of business the network connectivity between Company D and its bandwidth supplying company was overlooked. The company had since put in additional lines allowing immediate fail over in the event that one line goes faulty.

The BCP and Risk Manager highlighted the disastrous impact on the company’s reputation as well as financial impact as many businesses had SLA’s in place with their clients.

Table 16 below is a summary of the answers of the BCP and Risk manager.

Table 16: Summary of answers (Company D)

Questions	Answers
1. Does the company have a written business continuity plan?	Yes

2. Where is it kept and who has access to this document?	Kept on SharePoint so that anyone in the company can access it. Key players. Senior managers.
3. Are there any exclusions to your BCP such as personnel, natural disasters, and why?	Yes, Lack of additional personnel. Not sufficient business and technical staff involve in the plan. Location for staff to operate from.
4. Does the DRP form part of the BCP or is it a separate plan altogether?	The DRP within the BCP covers the technical aspects. Separate plans that makes up a BCP. DRP is covered by IT and Operations. BCP is enterprise wide.
5. Does business continuity and disaster recovery readiness have support of top management in your organization, if no why?	Yes, Top management just approve the budget, but aren't really concern about BCP. Top management does not fully understand the importance of BCP.
6. What happens if key personnel are not available during a disaster?	Nothing, there aren't any support from vendors. No support from any outsources companies. All applications are developed in house to meet business specific requirements therefore systems are unique to business.
7. Have your organization identified which vendors may need access to your facility after a disaster?	Yes only for specific vendors.
8. How often is the BCP reviewed and updated?	Real time replication, that allows all new applications to be included automatically. No formal review. BCP and DRP are treated as live documents and are updated as and when new requirements are presented.
9. How is business critical applications identified?	By the use of a scorecard. Owners of the application are responsible for the server on which the applications reside.

10. Who is responsible for identifying these applications?	Manager of the department in which the application reside. Information and security team.
11. Was your disaster covered by your plan, if no why?	**No, not really. We weren't able to effectively get hold of that particular vendor and we haven't identified the redundancy that we required, therefore it was not part of the plan**
12. Do you perform back-ups faithfully and include every server and hard disk?	No, test servers. Real time replication.
13. How often do you perform a BCP test? If tested, did you pass your test?	Some applications are tested quarterly. Tests are performed on a departmental basis.
14. Do you have unscheduled BCP test? If yes, did you pass your test? If no, why?	Yes when new changes take effect.
15. Does the company BCP highlight what are acceptable downtimes?	Yes, uptime is 99%
16. Do you feel that these times are attainable?	Yes, Due to the nature of our business we need to be up all the time.
17. What was the impact of the disaster on business?	SLA was missed with business. Possibility of losing clients. Reputation was damaged.

The answers to question 11 in Table 16 above is an indication that Company D did not perform a proper analysis of all its equipment and peripherals, thereby causing them to overlook a network connection that was relevant to their daily operations and that of their clients.

Questions 2, 5, 6, 8, 9, 13 & 15 in the above table are specifically linked to the key elements of an effective BCP as depicted in Section 2.1.3 of the literature review chapter. The purpose for these questions was to determine whether Company D had applied the key elements of a BCP.

Table 17 below is an analysis of the answers to the questions which relate to the key elements of an effective BCP as shown in Section 2.1.3 of the Literature Review Chapter

Table 17: Analysis of Company D's responses to research question linking to BCP Elements

Questions	Responses	Comply with key elements of an effective BCP as per Section 2.1.3
2. Where is the company's BCP kept and who has access to this document?	"Kept on SharePoint so that anyone in the company can access it. Key players. Senior managers".	Before a plan can be tested, employers and employees need to be familiar with the content of the plan and their role in the response and recovery. This can be done by reading through the plan together and discussing how you would apply it to a fictional scenario.
5. Does business continuity and disaster recovery readiness have support of top management in your organization?	"Yes, Top management just approve the budget, but aren't really concern about BCP. Top management does not fully understand the importance of BCP".	Get senior management involved and keep them committed.
6. What happens if key personnel are not available during a disaster?	"Nothing, there aren't any support from vendors. No support from any outsources companies.	In order for a plan to succeed, there must be multiple agency cooperation and

	All applications are developed in house to meet business specific requirements therefore systems are unique to business”.	involvement.
8. How often is the BCP reviewed and updated?	“Real time replication, that allows all new applications to be included automatically. No formal review. BCP and DRP are treated as live documents and are updated as and when new requirements are presented”.	Keep the plan current – Update the plan as applications gets updated
9. How are business critical applications identified?	“By the use of a scorecard. Owners of the application are responsible for the server on which the applications reside”.	Identify critical businesses and supporting functions and perform business impact analyses.
13. How often do you perform a BCP test? When tested, what were the results?	“Some applications are tested quarterly. Tests are performed on a departmental basis”.	Test the business recovery process and evaluate test results
15. Does the company BCP highlight what are acceptable downtimes?	“Yes, uptime is 99%”	Identify your recovery point objective (RPO) and recovery time objective (RTO), making sure your data protection solutions can meet these requirements.

The answers to questions 2, 5, 6, 8, 9, 13 and 15 in Table 17 above highlights that most of the key elements of a BCP had been adhere to by Company C.

5.3 Major Cause of Prolonged Downtime as per Company

Table 18 below is a summary of the primary reasons for the prolonged downtime during the respective disasters experienced by each of the four companies that were researched.

Table 18: Reasons for the prolonged downtime per company

Companies	Summary of reason of failure
Company A	The supply of electricity had been taken for granted and therefore never included it into the BCP.
Company B	The inclusion of routers was **overlooked** and therefore never tested.
Company C	All critical elements within an application were **overlooked** and not fully monitored therefore was never tested.
Company D	Redundancy for that connection was not identified or that network connection was **overlooked**.

If we consider the responses for each company in Table 18 above, there is a commonality in that most of the companies (company B to D) overlooked hardware peripherals namely a router and a network connection as well as software peripherals which is the service responsible for allowing an application to operate. To overcome the “overlooking” factor the companies that were researched should definitely consider incorporating another step in the Common BCP Process (Figure 8 in the Literature Review Section). This new step would include “identifying critical points of failure” and should include checking all aspects and include various software and hardware technical department heads that are responsible for their area of expertise. Each department head should then sign off his area and be involved in the testing phase of the Common BCP Process and signoff that their area has been tested. The new step namely “identifying critical points of failure” would be incorporated between the “BIA” phase and the “Develop a BCP” in the Common BCP Process. The reasons for BCP failure is highlighted in table 18 and can contribute directly to the disaster events in section 2.4 of the literature review chapter.

In the following chapter we will look at a model that will assist these companies and possibly other companies in South Africa to have a reduced or no downtime during a disaster.

CHAPTER 6: CONCLUSION AND RECOMMENDATIONS

The aim of this research was to determine why companies that had BCP in place still experienced prolonged downtime during a disaster. The extensive literature covered in chapter 2 highlights the different types of disaster events, key elements of an effective BCP and the factors that cause BCP failure.

Due to all the integrations of systems, most companies have come to realize that their business is now more dependent on IT than ever before and that greater focus should be placed on BCP to ensure that companies do not experience prolonged downtime during a disaster. Companies should strengthen their BCP and close any loop holes that might exist.

The companies that were studied and possibly many other companies that have a BCP in place, have realised that certain elements or criteria do not exist within their BCP thus causing them to experience prolonged downtime during a disaster.

Following the results of the research conducted with the four companies based within the Western Cape, it is evident that there is a vital gap within their BCP Process. If we compare the Common BCP Process as shown in Figure 14 below to that of BCP Process Model F Figure 15 below, it becomes apparent that an additional step has been added. This step is the step that was mentioned in the above Chapter in section 5.3 as “identifying critical points of failure”.

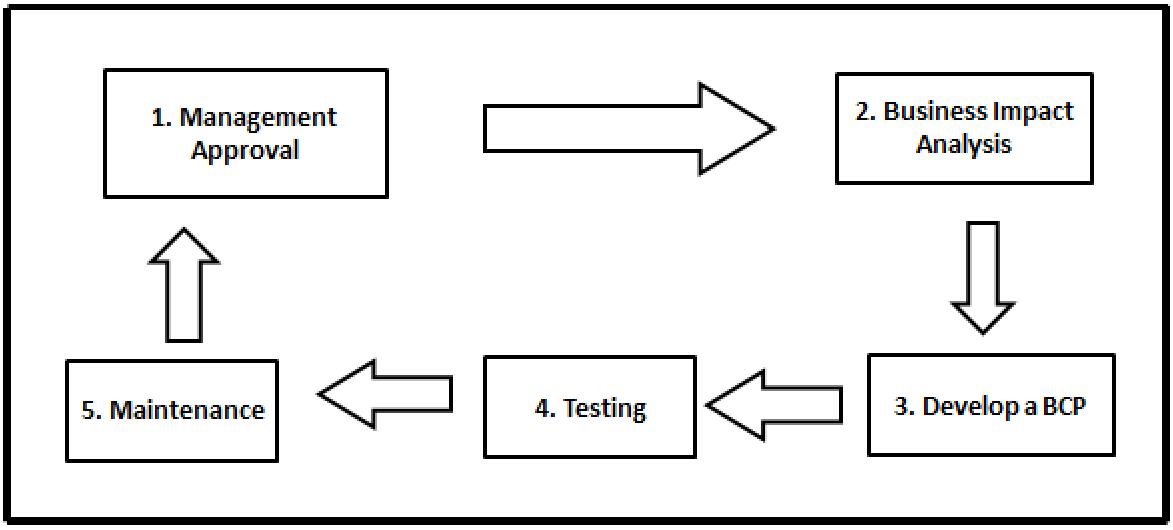

Figure 14: Common BCP Process

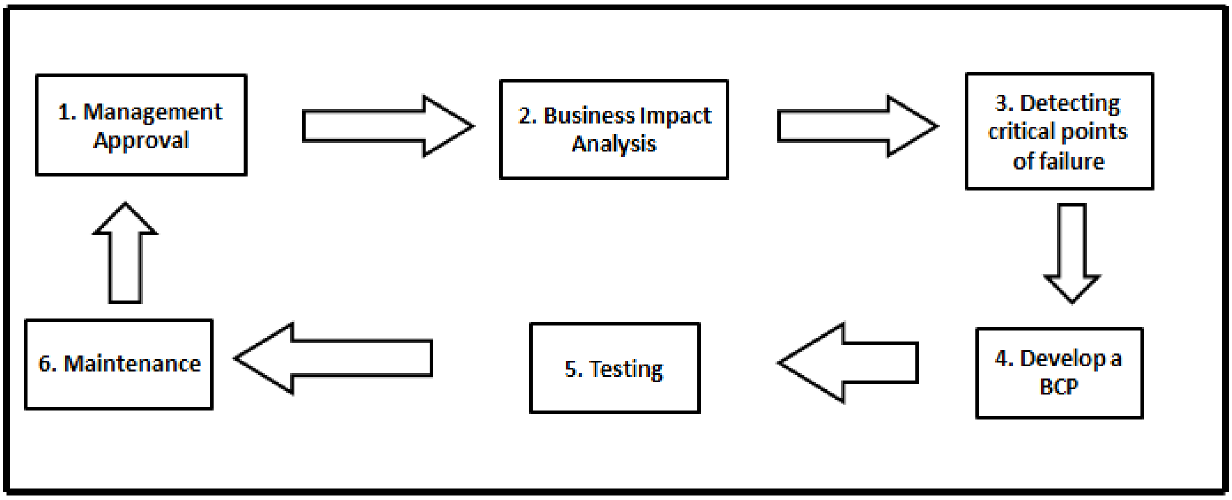
1. Management Approval
2. Business Impact Analysis
3. Detecting critical points of failure
4. Develop a BCP
5. Testing
6. Maintenance

Figure15: Proposed BCP Process Model F

In addition point 3 “Detecting critical points of failure” should be expounded as follows:

1. Create a detailed architectural diagram highlighting each possible point of failure. This should be done on a software and hardware level, thus involving the Application Manager as well as the Technical Manager.
2. Identify, test and sign off on each point of failure based on the architectural diagram.
3. Rank and rate each point of failure, so that only significant points of failure are incorporated into the final BCP document.

It is with great expectation that once the missing step is incorporated that companies might have less if any downtime during a disaster. In summary, table18 highlights the key reasons for the prolonged downtime during a disaster event and figure 15 can assist companies in bridging the gaps in their BCP development.

6.1 Research Limitation

This study adopted a qualitative approach which resulted in subjective opinions of the individuals that were interviewed being formulated. The main limitation of this study is that most of the companies that were studied are based within the Western Cape. A further constraint is that only private and public companies were studied and no NGO's and or Government Departments were involved. These limitations therefore allow a person to further investigate the scope of this research to the other provinces as well as studying NGO's and various Government departments.

6.2 Research Value

Many companies rely on the ability to conduct business continuously without missing any SLA's, as this could have a financial impact on them. Service orientated companies rely on their operations to have 99% uptime. Failing to do this, could result in their clients to seek a company that can offer them reliable and uptime service.

Table 18 in Chapter 5 proves that companies can experience prolonged downtime during a disaster by overlooking certain factors. In order to prevent companies from overlooking certain factors, it is therefore recommended that the additional step in Figure 15 above should be included in a common BCP process in future literature as this could ultimately improve BCP process for companies nationally within South Africa and even worldwide.

REFERENCES:

Aggelinos, G. & Katsikas, S.K. (2011). “Enhancing SSADM with disaster recovery plan activities” Information Management & Computer Security, pages 248-261

Aleem, A. and Antwi-Boasiako, A. (2011), “Internet auction fraud: the evolving nature of online auctions criminality and the mitigating framework to address the threat”, International Journal of Law, Crime and Justice, September (special edition Fraud Management)

Alavi, M. & Carlson, P. (1992). “A Review of MIS Research and Disciplinary Development”. Journal of Management Information Systems.

Aliaga, M. & Gunderson, B. (2002) “Interactive Statistics.” [Thousand Oaks]: Sage

Al-Zahrani, A (2009) “Decision making assessment model throughout IT Business Continuity Planning (BCP) Lifecycle in small or medium-size organizations in Saudi Arabia” Open University Malaysia.

Babbie, E & Mouton, J. (2002). “The practice of social research”. Cape Town: Oxford University Press.

Bajgoric, N & Moon, Y.B (2009) “Enhancing system integration by incorporating business continuity drivers” Vol. 109

Bateman, I, Authors, L, Albon, S, Balmford, A, Brown, C, Church, A, Haines-young, R, Jules, N, Turner, K, Vira & B, Winn, J (2011). “Conceptual Framework and Methodology”

Baxter, P. and Jack, S. (2010) “Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers” McMaster University, West Hamilton, Ontario, Canada

Bell, J. (1993). “Doing Your Own Research Project: A Guide for First-Time Researchers in Education and Social Science”. Buckinghamshire, Open University Press.

Benbasat, I., Goldstein, D.K., Mead, M. (1997). ‘The Case Research Strategy in Studies of Information Systems”. 11(3) : 369-386.

Botha, J. & Von Solms, R. (2004). "A cyclic approach to business continuity planning". Information Management & Computer Security. Vol 12 No. 4. 328-337.

Bless, C., & Higson-Smith, C. (1995). “Fundamentals of research methods. An African perspective”. RSA: Juta.

Burns, N. & Grove, SK. (2005).”The Practice of Nursing Research: Conduct, Critique, and Utilization (5th Ed.)”. St. Louis, Elsevier Saunders

Byrne, M (2001) ”Ethnography as a qualitative research method” AORN Journal

Campbell, M. (2012). “Best Practices for Creating an Effective Business Continuity Plan” available on **http://esj.com/articles/2012/11/05/business-continuity-plan.aspx**

Camp, W. G. (2001). “Formulating and evaluating theoretical frameworks for career and technical education research”. *Journal of Vocational Education Research, 26* (1). Retrieved May 1, 2009 from: http://scholar.lib.vt.edu/ejournals/JVER/v26n1/camp.html

Cervone, H.F (2006). "Managing digital libraries: the view from 30,000 feet. Disaster recovery and continuity planning for digital library systems". OCLC Systems & Services. Vol. 22 No. 3. 173-178.

Chow, W.S. (2000) “Success factors for IS disaster recovery planning in Hong Kong”. Hong Kong Baptist University, Hong Kong.

Chow, W. S and Ha, W. (2009) “Determinants of the critical success factor of disaster recovery planning for information systems”. Journal: Information Management and Computer Security. Department of Finance and Decision Sciences, Hong Kong Baptist University, Kowloon Tong, Hong Kong, China

Clifton, R. (2000). “Business Continuity Planning” Occupational health & safety (Waco, Tex.)

Collis and Hussey (2003) “Business Research: A Practical Guide for Undergraduate and Postgraduate Students” Palgrave Macmillan, 2003

Creswell, JW. (1994). “Research Design: Qualitative & Quantitative Approaches”. United States of America: Sage Publications.

Dawson, C. (2002), “Practical Research Methods”, New Delhi, UBS Publishers’ Distributors,

De Vos AS. & Fouche, CB. (1998). “General Introduction to Research Design, Data Collection Methods and Data Analysis”. In De Vos (ed). Research at Grassroots. A primer for caring professions. Pretoria: Van Schaik Publishers.

Edwards, B (1994). “Developing a Successful Network Disaster Recovery Plan”. Information Management & Computer Security, Vol. 2 No. 3, 1994, pp. 37-42 © MCB University Press , 0968-5227

Erickson, F. (1986). “Qualitative Methods in Research on Teaching”. Wittrock (Ed.). New York: MacMillan.

Erlanger, L. (2006). "In case of emergency activate business continuity plan". InfoWorld. 27-31.79

Fade, S. (2004). “Using interpretative phenomenological analysis for public health nutrition and dietetic research: a practical guide”. Proceedings of the Nutrition Society, (63): 647-653

Gardener, N.J.L. (2010) “Business Continuity Psychology - From Strategy to Benefits?”

Gerring, J. (2004). “What is a case study and what is it good for?” *The American Political Science Review*, 98 (2): 341-354.
Available at:
http://ejournals.ebsco.com/direct.asp?ArticleID=PB1ADPV9TD9DTCRKJL0T.

Glenn, J. (2002), “What is business continuity planning? How does it differ from disaster recovery planning?”, Disaster Recovery Journal, available at: www.drj.com/articles/win02/1501- 14p.html (accessed 11 May).

Gordon, C. (2000), “How to cost-justify a business continuation plan to management”, Disaster Recovery Journal, available at: www.drj.com/articles/spring00/1302-05.html (accessed 7 March 2002).

Government of Canada Public and Safety. “A guide to business continuity planning” Retrieved on 2011-06-12 from **http://www.publicsafety.gc.ca/prg/em/gds/bcp-eng.aspx**

Grimaldi, R. (2002) “Why do Business Continuity Plans fail?” Journal: Risk and Insurance. Retrieved on 2011-10-20 from **http://www.rmmag.com/Magazine/PrintTemplate.cfm?AID=1483**

Hancock B, (2002), “Trent Focus for Research and Development in Primary Health Care: An Introduction to Qualitative Research.” Trent Focus, Harris, L. (2001). “Keeping IT alive when disaster strikes.” Retrieved on 2011-08-12 from http://www.itweb.co.za/index.php?option=com_content&view=article&id=44662&catid=116

Hearnden, K. (1995), “Business continuity planning: Part 4, Establishing business priorities”, Computer Audit Update, vol. 8, pp. 3 - 13.

Hellman, L & Magnus, K (2008) “A Disaster Recovery Planning Guide- On how to mitigate the supply chain disruption risks of a totally destroyed central warehouse” Department of Fire Safety Engineering and Systems Safety Lund University, Swede. Report 5282

Heng, G. M (1996) “Developing a suitable business continuity planning methodology” FBCI, CDRP Group Manager, Standard Chartered Bank

Hudic, A., Islam, S., Kieseberg, P., Rennert, S., Edgar R. Weippl, (2013),"Data confidentiality using fragmentation in cloud computing", International Journal of Pervasive Computing and Communications, Vol. 9 Iss 1 pp. 37 - 51

Ingenuity (2006) “Success or Failure? Your Keys to Business Continuity Planning” © 2000-2006, Ingenuity, Inc. White Paper available at http://www.teamingenuity.com/Sites/teamingenuity3/Documents/Technology/Ingenuity%20White%20Paper-%20Keys%20to%20BCP%20success.pdf

Islam, S., Mouratidis, H. and Ju¨rjens, J. (2011), “A framework to support alignment of secure software engineering with legal regulations”, Journal of Software and Systems Modeling (SoSyM), Theme Section on Non-functional System Properties in Domain-Specific Modeling Languages (NFPinDSML), Vol. 10 No. 3, pp. 369-94

Kaplan, B. and Maxwell, J.A. (1994) “"Qualitative Research Methods for Evaluating Computer Information Systems," in Evaluating Health Care Information Systems:

Methods and Applications", J.G. Anderson, C.E. Aydin and S.J. Jay (eds.), Sage, Thousand Oaks, CA, pp. 45-68.

Karakasidis, K. (1997). "A project planning process for Business Continuity." KPMG Information Technology Consulting Division, Melbourne, Australia
Lee T (2009) "Using ITIL to measure your Business Continuity" Trinity Consulting Solutions LLC

Kohlbacher, F. (2005). "The use of qualitative content analysis in case study research". Forum: Qualitative Social Research, Art. 21 (12/05). Available at: http://www.qualitaqtive-research.net/fqs-texte/1-06/06-1-21-e.htm

Lastrucci, C.L. (2002) "The Scientific Approach: Basic Principles of the Scientific Method" Science; Methodology, 257p

Imai, M., (1986), Kaizen. New York: McGraw Hill Publishing

Langley, E. (2010) "Business Continuity - Establish Recovery Point and Time Objectives" http://community.spiceworks.com/how_to/show/1676-business-continuity-establish-recovery-point-and-time-objectives
Levinson, V. (2012). "Disaster Recovery and Business Continuity Planning" Lesson we need to learn from Sandy. http://blog.primetelecommunications.com/2012/11/12/disaster-recovery-and-business-continuity-planning-lessons-we-need-to-learn-from-sandy/

Lindström, J., Samuelsson, S. & Hägerfors, A. (2010). "Business continuity planning methodology." Disaster Prevention and Management, 19(2), pp.243-255. Available at: http://www.emeraldinsight.com/10.1108/09653561011038039 [Accessed June 17, 2011].

Maslen, C. (1996). "Testing the plan is more important than the plan itself". Business Recovery, Optus Communications

Marzanah A. J. (2009). "An investigation into methods and concepts of qualitative research in information research". Computer and information science 2 (4) Available at http://www.ccsenet.org/journal/index.php/cis/article/view/3200/3714

Mercer, V. N. (2001). "The double-edged sword: examining perceptions of technology as a process of enablement and construct within an academic organization". *Unpublished MA thesis*, University of North Carolina, October 2001.

Meyer, D.Z. & Avery L.M. (2008). "Excel as a Qualitative Data Analysis Tool" first published on September 20, 2008

Molinari, A (2010) "Top 10 Reasons Business Continuity and Disaster Recovery Plans Fail" Business Continuity Management Professionals

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

Morwood, G. (1998), "Business continuity: awareness and training programmes", Information Management & Computer Security, Vol. 6 No. 1, pp. 28-32.

Mouton, J. (1996). "Understanding social research". RSA: J.L van Schaik.

Mouton, J. (1998), "Patterns of Research Collaboration in Academic Science in South Africa". Lisbon, EASST.

Murphy E., Dingwall R., Greatbatch D., Parker S. & Watson P. (2007). "Qualitative research methods in health technology assessment: a review of the literature", School of Sociology and Social Policy, University of Nottingham, Nottingham, UK

Myers, M. D. 1994. A disaster for everyone to see: an interpretative analysis of a failed IS project. Accounting, management and information technology, 4(4): 185-201 Elsevier Science.

Myers, M.D. (2009) “Qualitative Research in Business & Management”. Sage Publications, London

Neale, P., Thapa, S. & Boyce, C., (2006). “PREPARING A CASE STUDY : A Guide for Designing and Conducting a Case Study for Evaluation Input.” Pathfinder International Tool Series, Monitoring and Evaluation – 1

Nickolette, C. and Schmidt, J. (2001) “Business Continuity Planning – Description & Framework”. Business Continuity Planning white paper.

Nishchal, N. and Mathur, P. (2010), “Cloud computing: new challenge to the entire computer industry”, Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference, pp. 223-8

Noakes-Fry, K. (2001) “Business Continuity and Disaster Recovery Planning and Management: Perspective” Technology overview

Pather, S. & Remenyi, D. (2005). Some of the philosophical issues underpinning research in Information Systems-form positivism to critical realism. South African Computer Journal, No 35.

Patton, E, Appelbaum, S.H. (2003). “The case for case studies in management research”. *Management Research News*, 26(5): 60-71
Available at
http://ejournals.ebsco.com/direct.asp?ArticleID=BDT0JKNLA89JLAQ51YCC

Pit, M. & Goyal, S. (2004). "Business continuity planning as a facilities management tool". Facilities. Vol 22 No 3/4. 87-99.

Phelps, N. (1986). “Setting up a crisis recovery plan”. The Journal of business strategy

Planning , B (2000). “Introduction to Business Continuity Planning”. SANS Institute InfoSec Reading Room.

Priest, H. & Roberts, P. (2010). “Gathering and making sense of words”. In Roberts, P. and Priest, H. (2010) Healthcare research A handbook for students and practitioners, Wiley-Blackwell, UK [Scholar Google e-book]. Rapoport, R.N.(1970) “Three Dilemmas in Action Research”, Human Relations (23:6), pp. 499-513.

Proofpoint (2010), “Outbound email and data loss prevention in today’s enterprise”, Tech. Report, Proofpoint.

Rosenberg, N. (2010). “10 Steps to Implement a Disaster Recovery Plan” From the QTS White Paper Series

Rothstein Associates (2008), “Statistics and surveys-genera industry statistics”, available at: www.rothstein.com/links/rothstein_recommended32.html (accessed 2 May 2008).

Rozek, P. and Groth, D. (2008), “Business continuity planning. It's a critical element of disaster preparedness. Can you afford to keep it off your radar?” Health Management Technology. Vol 29

Rudestam, K. E. & Newton, R. R. (1992) Surviving your dissertation (London, Sage).

Savage, M. (2002) “Business Continuity Planning” Journal: Work Study

Sayen Organisation (2008) “Understanding Disasters” Internship Series, Vol. 3 available at http://www.sayen.org/Volume-III.pdf

Semer, L.J. (1998), “Disaster recovery planning for the distributed environment", Internal Auditor, Vol. 55 No. 6, pp. 41-7.

Singleton, R.A *et al*. (1993). “*Approaches to social research”* (2nd ed) Oxford University Press.

Smit, N. (2005) “Business Continuity Management – A Maturity Model” Master’s Thesis Informatics and Economics

Smith, J. A., Flowers, P. & Larkin, M. (2009). “Interpretative Phenomenological Analysis: theory, method and research”. UK: Sage Publishers.

Snoyer, R.S and Fischer, G.A (1993), “Managing Microcomputer Security”, Business One, Irwin, Homewood, IL, p. 431.

Sommer, R. & Sommer, B. (2002). “A practical guide to behavioral research: tools and techniques” Oxford University Press, Incorporated, 2002

Swanson, M., Lynes, D., & Gallup, D. (2010), “Contingency Planning Guide for Federal Information Systems”. Nist Special Publication 800 – 34 Rev 1.

United States General Accounting Office (1999), Year 2000 Computing Crisis: Business Continuity and Contingency Planning, available at: www.gao.gov/special.pubs/ ai10119.pdf (accessed 23 October 2000).

Wan, S. (2009) “Service impact analysis using business continuity planning processes” Campus –Wide Information Systems

Willig, C. 2001. Introducing qualitative research in psychology: adventures in theory and method, Buckingham: Open University Press.

Wilson, B. (2000), “Business continuity planning: a necessity in the new e-commerce era”, Disaster Recovery Journal, available at: www.drj.com/articles/fal00/1304-02.htm (accessed 21 October).

World Medical Association (WMA) (2010), WMA Statement on Medical Ethics in the Event of Disasters, available at: www.wma.net (accessed August 16, 2012).

Wyckoff, K (2007) “Tips on Qualitative and Quantitative Data Collection Methods”.

Yin, Robert, K. (1994). “Case study research: Design and methods”, 2nd ed. Thousand Oaks, CA: Sage.

Yin, R. K. (1984). “Case study research: Design and methods”. Newbury Park, CA:

Yin, R.K (2003), “Case Study Research: Design and Methods”, Sage Publications, Inc, 3rd edition

Zainab, A.N., Chong, C.Y. and Chaw, L.T. (2013),"Moving a repository of scholarly content to a cloud", Library Hi Tech, Vol. 31 Iss
2 pp. 201 - 215

APPENDICES:

Appendix 1: Questionnaire

UNIVERSITY of the
WESTERN CAPE

Research Questionnaire for Master's Degree in Information Management

Reasons and identifying Business Continuity Plan failure after a disaster event

Research conducted by Fadeel Sambo

By participating in this research you declare that all information provided is true and accurate and can be used for the purpose of this research. Due to the nature of the interview and questions this interview will be recorded and transcribed at a later stage.

May I proceed with this interview and do you agree to the above declaration □Yes

Name of Company: ______________________________________

Name of respondent: ______________________________________

Contact Details: (w)______________________________________

cell______________________________________

Email:____

Department: ____

Position held within the company:___________________________

Signature of Respondent: ________________________________

1. Does the company have a written business continuity plan?

2. Where is the company's BCP kept and who has access to this document?

3. Are there any exclusions to your BCP such as personnel, natural disasters, and why?

4. Does the DRP form part of the BCP or is it a separate plan altogether?

5. Does business continuity and disaster recovery readiness have support of top management in your organization? And if not why?

6. What happens if key personnel are not available during a disaster?

7. Has your organization identified which vendors may need access to your facility after a disaster?

8. How often is the BCP reviewed and updated?

9. How are business critical applications identified?

10. Who is responsible for identifying these applications?

11. Was your disaster covered by your plan, if no why?

12. Do you perform back-ups faithfully and include every server and hard disk?

13. How often do you perform a BCP test?

14. Do you have unscheduled BCP test? If tested, did you pass your test?

15. Does the company BCP highlight what are acceptable downtimes after specific disasters?

16. Do you feel that these times are attainable?

17. What was the impact of the disaster on business?

Appendix 2: Summary of Questionnaire

In the tables below the companies will be abbreviated as follow:

- Company A (A)
- Company B (B)
- Company C (C)
- Company D (D)

Summary per question:

Table 2: Question 1

Question 1. Does the company have a written business continuity plan?				
Answers	**A**	**B**	**C**	**D**
Yes	X	X	X	X

Summary for Table2:

Each company that were interviewed has a written BCP. This was a prerequisite to continue with the interview

Table 3: Question 2

Question 2. Where is the company’s BCP kept and who has access to this document?				
Answers	**A**	**B**	**C**	**D**
Kept on share-point for the whole company to view	X	X	X	X
The complete IT department	X	X		
At the Disaster Recovery Site	X	X		
Key players				X
Senior managers				X

Summary for Table3:

Every company that was interviewed has a copy of their BCP on a Share-point portal, thereby allowing every employee to view and familiarize themselves with the BCP procedures. Some companies has there BCP document stored at their Disaster Recovery Site, so that policies and procedures can be followed during the disaster.

Table 4: Question 3

Question 3. Are there any exclusions to your BCP such as personnel, natural disasters, and why?				
Answers	**A**	**B**	**C**	**D**
Yes	X	X		X
Lack of additional technical personnel.	X	X		X
Unlikely events such as floods, tornadoes and so on.	X			
Non critical business applications due to budget constraints.	X			
Power failures as company is on the same sub-station as parliament and the chances that parliament would experience a power failure is very slim	X			
Not sufficient business staff involve in the plan, mainly for testing	X	X		X
No			X	
Everything is covered			X	
Location for staff to operate from				X

Summary for Table4:

Majority of the companies that were interviewed had exclusions and the most common exclusions were

- The lack of additional technical personnel
- Not sufficient business personnel involved in the testing process

Table 5: Question 4

Question 4. Does the DRP form part of the BCP or is it a separate plan altogether?				
Answers	**A**	**B**	**C**	**D**
The DRP is part of the BCP	X		X	
The DRP consist within the BCP		X		
The BCP covers all the natural disasters			X	
The DRP within the BCP covers the technical aspects			X	X
Separate plans that makes up a BCP				X
DRP is covered by IT and Operations				X

BCP is enterprise wide				X

Summary for Table5:

All of the companies that were interviewed have a DRP as part of their BCP. Even though some companies have separate individual plans it still formed part of the BCP as a whole.

Table 6: Question 5

Question 5. Does business continuity and disaster recovery readiness have support of top management in your organization, if no why?				
Answers	**A**	**B**	**C**	**D**
Yes	X	X	X	X
There is a committee that monitors all the BCP Tests	X			
There is a Business Continuity Management (BCM) team that looks after enterprise wide BCP			X	
Top management just approve the budget, but aren't really concern about BCP				X
Top management does not fully understand the importance of BCP	X			X

Summary for Table6:

All the companies that were interviewed has the support of top management within the organization, however for some of the companies that were interviewed, their top management don't fully understand the importance of a BCP.

Table 7: Question 6

Question 6. What happens if key personnel are not available during a disaster?				
Answers	**A**	**B**	**C**	**D**
Vendors are on standby to assist	X	X	X	
Support from vendors		X	X	
There is an agreement with third party vendors for technical support in the event of a disaster		X		

All key personnel has alternative numbers from a different service provider			X	
All critical services have standby and escalation procedures in place			X	
Nothing, there aren’t any support from vendors				X
No support from any outsource companies				X
All applications are developed in house to meet business specific requirements therefore systems are unique to business				X

Summary for Table7:

Majority of the companies that were interviewed has vendors on standby to assist them on their applications in the event of a disaster. One company however has no support from vendors as all the applications are developed in-house.

Table 8: Question 7

Question 7. Have your organization identified which vendors may need access to your facility during a disaster?				
Answers	**A**	**B**	**C**	**D**
Yes only for specific vendors	X	X	X	X
Service Level Agreements (SLA) are in place with specific vendors			X	

Summary for Table8:

All the companies that were interviewed has identified and allowed for vendors to access their disaster facility. Some even went to the extent of getting an SLA in place with vendors.

Table 9: Question 8

Question 8. How often is the BCP reviewed and updated?				
Answers	**A**	**B**	**C**	**D**
Every 6 months	X		X	
Annually		X		
Real time replication, that allows all new applications to be included automatically		X	X	X
Some critical applications are reviewed quarterly			X	
No formal review				X
BCP and DRP are treated as live documents and are updated as and when new requirements are presented				X

Summary for Table9:

Majority of the companies that were interviewed has real time replication, thereby allowing that all new applications are implemented immediately. Some companies also review and update there BCP every 6 months.

Table 10: Question 9

Question 9. How are business critical applications identified?				
Answers	**A**	**B**	**C**	**D**
Through general consciences among IT and Business	X			
No specific Business Impact Analysis Tools	X			
By the use of a matrix		X	X	X
A Business Impact Analysis Tool is used to determine the impact of each application		X		
All business critical services and systems are rated as per criticality. (Mission critical, business critical, non-critical)			X	
Owners of the application are responsible for the server on which the application reside				X

Summary for Table10:

Most companies that were interviewed use a matrix to calculate and identify critical business applications.

Table 11: Question 10

Question 10. Who is responsible for identifying these applications?				
Answers	**A**	**B**	**C**	**D**
IT	X			
Business	X			
Each business unit will sign off on their own application		X	X	
Business owner			X	
BCM Team			X	
Manager of the department in which the application reside				X
Information and security team				X

Summary for Table11:

Of the companies that were interviewed, business units, business owners, business continuity management team and departmental mangers signs off or take responsibility for the applications.

Table 12: Question 11

Question 11. Was your disaster covered by your plan, if no why?				
Answers	**A**	**B**	**C**	**D**
No	X	X	X	X
Our company shares the same sub-station as parliament and the chances that parliament would experience a power failure is very slim.	X			
Overlooked	X	X		X
It was not foreseen due to information not being available as problem was intermittent			X	

Summary for Table12:

None of the companies that were interviewed had there disaster covered in there plan and the reason was that they overlooked that aspect within the BCP.

Table 13: Question 12

Question 12. Do you perform back-ups faithfully and include every server and hard disk?				
Answers	**A**	**B**	**C**	**D**
No	X	X	X	X
Budget constraints due to the size of data that will be safe to disk. Disks are expensive	X			
Test servers	X	X	X	X
Non critical business applications	X	X		
All business critical servers are backed up on a daily basis	X	X	X	
Real time replication		X	X	X

Summary for Table13:

Each company that was interviewed do not backup every hard disk and server. Test servers and non-critical business applications are not backed up, however critical business servers are backed up on a daily basis through real time replication.

Table 14: Question 13

Question 13. How often do you perform a BCP test? When tested, what were the results?				
Answers	**A**	**B**	**C**	**D**
Every 6 months	X	X	X	
No not all the time	X	X	X	
Once a year an ICT test is performed. This is a technical test to ensure that we are able to restore all servers.		X		
A user test is done once a year to ensure that all applications restored are fully operational		X		
Some applications are tested quarterly			X	X
Insufficient disk space on server			X	
Test are performed on a departmental basis				X

Summary for Table14:

Of the companies that were interviewed, majority of them perform a BCP test every 6 months and do not always pass each BCP test.

Table 15: Question 14

Question 14. Do you have unscheduled BCP test? If tested, did you pass your test?				
Answers	**A**	**B**	**C**	**D**
No	X	X	X	
Too expensive	X			
Testers need to be arranged before the time.	X	X	X	
Company is not ready for it		X		
Yes would like to do unscheduled tests		X		
Yes when new changes takes effect				X

Summary for Table15:

Majority of the companies that were interviewed do not perform unscheduled BCP test as testers needs to be arranged before the time.

Table 16: Question 15

Question 15. Does the company BCP highlight what are acceptable downtimes?				
Answers	**A**	**B**	**C**	**D**
Yes	X	X	X	X
Form part of the BIA		X		
Uptime is 99%			X	X

Summary for Table16:

All the companies that were interviewed have acceptable downtimes documented within the BCP.

Table 17: Question 16

Question 16. Do you feel that these times are attainable?				
Answers	**A**	**B**	**C**	**D**
Yes	X	X	X	X

Time frames has been thoroughly tested and agreed upon			X	
Due to the nature of our business we need to be up all the time			X	X

Summary for Table17:

All the companies that were interviewed feels that the downtime is attainable, even though majority of them has 99.9% uptime.

Table 18: Question 17

Question 17. What was the impact of the disaster on business?				
Answers	**A**	**B**	**C**	**D**
SLA was missed with business	X	X		X
Retail outlet had to trade manually as databases resides at head office	X			
No stock updates were sent to and fro from retail outlet	X			
Only cash transactions	X			
Clients could not trade		X		
Financial impact		X		
Possibility of losing clients		X	X	X
Entire call centre was down			X	
Reputation was damaged				X

Summary for Table18:

Most of the companies that were interviewed missed Service Level Agreements with business and the possibility of losing clients due to their unforeseen disaster.