Spring 4-12-2016

A PROCESS MODEL FOR ICT BUSINESS CONTINUITY PLAN FOR DISASTER EVENT IN SOUTH AFRICA SMALL AND MEDIUM ENTERPRISES (28)

Felix Olu Bankole
University of South Africa, olu.bankole@gmail.com

Fadeel Sambo
University of the Western Cape

A Process Model for ICT Business Continuity Plan for Disaster Event in South Africa Small and Medium Enterprises

Felix Olu Bankole[1], Fadeel Sambo[2]
[1] School of Computing, University of South Africa, South Africa
[2] Information Systems, University of the Western Cape, South Africa

Small and Medium Enterprises (SMEs) are expose to the risks of business interruption as they expand and become more dependent on Information Communication Technology (ICT) infrastructure. The current study seeks to determine why organization that have Business Continuity Plan (BCP) in place and implement regular testing of their plan still experience prolong downtime during a disaster event resulting in Service Level Agreement (SLA) not being met or major financial loss.

By employing a descriptive analytics approach through a qualitative case study, the research propose a normative process model for comprehensive procedures of BCP for business leaders, ICT service managers, IS executives, data science researchers, risk managers, entrepreneur and policy makers on how to adopt strategies on effective disaster risk reduction and management in SMEs. The current study offer both theoretical and practical implications for BCP in SMEs.

Keywords: Business Continuity Plan, Disaster, SMEs, Risk, South Africa, Data Analytics

1. INTRODUCTION

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 and Schmidt, 2001). The use and adoption of ICT service management in organization has created a considerable amount of Computer Information Systems that process, transmit and store information (Botha and Von Solms, 2004).

Individual organization is unique, and as such will have a distinctive BCP, irrespective of similarities within industries and variations in organizational landscape (Cerullo and Cerullo, 2004) because an ICT failure or disaster would create great consequences for organization.

A BCP is a document that consists of collection of different procedures and information which is developed and maintained to be used in the event of an emergency or disaster (Rozek & Groth, 2008).

It is also considered as a process that ensures that operations and services are uninterrupted for the end-users or customers in an organization (Gibb and Buchanan, 2006). The risk of business interruption in Small and Medium Enterprises (SMEs) expand as organization depends on ICT infrastructure services, therefore comprehensive procedures for BCP plan to mitigate against interruption of the business systems is required (Cerullo and Cerullo, 2004).

SMEs are playing an ever-increasing role in innovation, poverty alleviation and socio-economic development (OECD, 2010). This is driven by changes in ICT technologies and markets. The spin-offs and high growth businesses are having remarkable success and consequently adding value to socio-economic development. However, SMEs are susceptible to disaster unless they prepare in advance for their operations processes (Webb, Tierney and Dahlhamer, 1999).

The causes of business interruption in SMEs are not mainly from natural disasters but are multifaceted such as human errors in the systems, power outages and malicious threats (Gibb and Buchanana, 2006; Cerullo and Cerullo, 2004). For example, in the UK, there was Cyber extortion in which a distributed denial of service attack on online gaming companies occurred (Paulson and Weber, 2006), in the US, the Worldpay experienced a denial of service attack as a result of generated e-mail (Computer Crime Research Center, 2003; Gibb and Buchanan, 2006) and other disruptions, in Australia and New Zealand.

The major focus of BCP is on failure prevention by using predictive analytics techniques to identify risks and putting procedures in place to ensure that business functions are continuously operational. However, the current research employs a descriptive analytics since SMEs that have BCP still experience downtime to provide insight into the past and understand how they might influence future outcomes. Therefore, the research applied two-phased analytics approach-descriptive and prescriptive.

Crisis or disaster event in an organization could possibly be any emergency that suddenly occurs and that disrupts day to day operations of the business, which could damage a company's competitive advantage, thereby requiring immediate attention (Phelps, 1986). Other aspects such as technological disasters, riots and human carnage, terrorisms, climate change and so on has over the years played an equal if not larger share in disasters (Sayen, 2008).

The development of BCP has been a critical problem for most SMEs and little literature that focus on BCP management for SMEs existed (Weems, 1991; Botha and Von Solms, 2004). Though, South African organizations tend to be relatively strong in the field of Disaster Recovery and Planning (DRP), they are not as good as it should be at Business Continuity Planning (BCP) and most of their approach is reactive rather than proactive (Harris, 2001).

To overcome the downtime being encountered daily by the organizations using the traditional DRP approach, a more comprehensive and rigorous BCP is needed to achieve a state of business continuity where critical systems and ICT networks are continuously available. Many businesses today require 24 hours and 7 days a week operations in order to survive, as a single downtime might mean the difference between financial gain and financial loss. Therefore with the ever increasing dependency on I**CT** services in Small to Medium Enterprises (SMEs), it has become a business requirement that systems be fully operational even during a disaster by adopting a **Computer Information Systems** architectural model that would curb disasters in a typical business enterprise.

This study explores a business continuity service plan model for disaster event in SMEs in organization. The research question focus on the type of BCP service required for management of disaster in SMEs

The research would provide a comprehensive procedures of BCP plan for Business leaders, risk managers, entrepreneur and policy makers on how to adopt strategies on effective disaster risk reduction and management.

The rest of the paper is organized as follows: Section 2 introduces the conceptual background. Section 3 provides an overview of BCP procedural process. Section 4 presents the research focus. In Section 5, the conceptualization of BCP processes is presented. Data analysis and results are discussed in Section 6 and Section 7 the conclusion and discussion.

2. CONCEPTUAL BACKGROUND

The frequent community-wide disasters, as well as unusual disasters that corporations, institutions, municipalities and government agencies have suffered in the past years have revealed that planning for disaster recovery is not enough to control these unforeseen circumstances. There must be adequate plan for business continuity (Moore, 1995). Disasters occur for a number of reasons, both routine and dramatic, and BCP must address every aspect of these incidents (Cervone, 2006). This seeming unpredictable impacts and uniqueness of the incidents demands dynamic, real time, effective and cost efficient solutions hence making BCP suitable for ICT service management research. The need to evaluate how organizations can prevent recurring of disaster event by implementing proper BCP so as to ensure minimal downtime and business impact are essential (Grimaldi, 2002).

It is therefore imperative to ensure that the correct procedures, policies and plans are in place to protect an organisation's ICT infrastructure and data. For example, creating a redundancy for backup and restore of organization's data are crucial for continuity in the event of a disaster as a means of contingency planning (CP). Contingency planning is the procedure developed to explore and prepare for any occurrence of eventuality (Kukalis, 1991).

Several scholars have examined the difference between BCP, DRP and Contingency Planning (CP). The inter-relationship of these three processes is illustrated in Figure 1 (Botha & Von Solms, 2004). The smaller circles labelled A to I represent various business processes. These processes are all dependant on services and infrastructure provided by IT section of an organization as depicted by the innermost circle in the figure. Some of these processes are also dependant on others, as depicted by adjacent circles. The outermost circle represents a combination of the disaster recovery plan for IT section of an organization and the contingency plans for these various business processes.

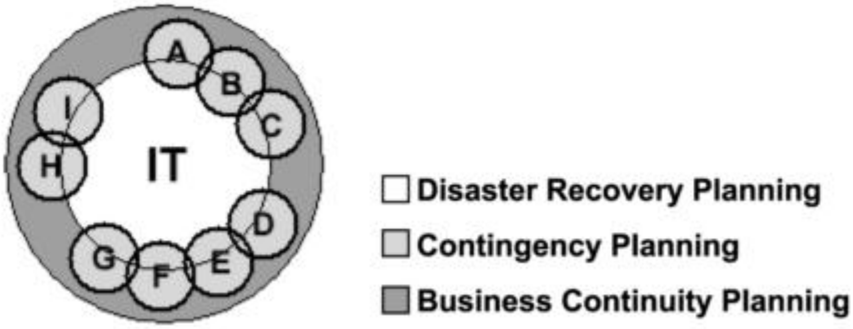

Figure 1: BCP, CP, DRP Relationship (Botha & Von Solms, 2004)

3. OVERVIEW OF BCP PROCEDURAL PROCESS

The key element in a BCP is the formation of the metrics of Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for data and applications which the IT section of an organization employs in creating their DRP and to configure their redundancy backups and offsite replication (Langley, 2010). Recovery time objective (RTO) is the length of time that it takes to recover from an outage (scheduled, unscheduled, or disaster) and to resume normal operations for an application or a set of applications. RTO is important for selecting appropriate technologies that are best suited for meeting the Maximum Tolerable Downtime (MTD) (Swanson, Lynes & Gallup, 2010).

In circumstances that, the RTO would not be met and the MTD is inflexible, there required an initiation of plan of action in the form of milestone to document the situation and plan for its mitigation.

The main 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); and the BCP process should comprise of certain components which should be used in conjunction with a risk management process, i.e. risk reduction programme by appropriating the following procedures: (Cerullo and Cerullo, 2004; Weems, 1991; Botha and Von Solms, 2004)
(i) Obtain top management approval and support (ii) Establish a business continuity planning committee (iii) Perform business impact analysis (iv) Evaluate critical needs and prioritize business requirements (v) Determine the business continuity strategy and associated recovery process. (vi) Prepare business continuity strategy and its implementation plan for executive management approval (viii) Prepare business recovery plan templates and utilities, finalize data collection and organize/develop the business recovery procedures. (ix) Develop the testing criteria and procedures. (x) Test the business recovery process and evaluate test results. (xi) Develop/review service level agreement (SLAs). (xii) Update/revise the business recovery procedures and templates.
The above statement are summarised and presented in Figure 2 below:

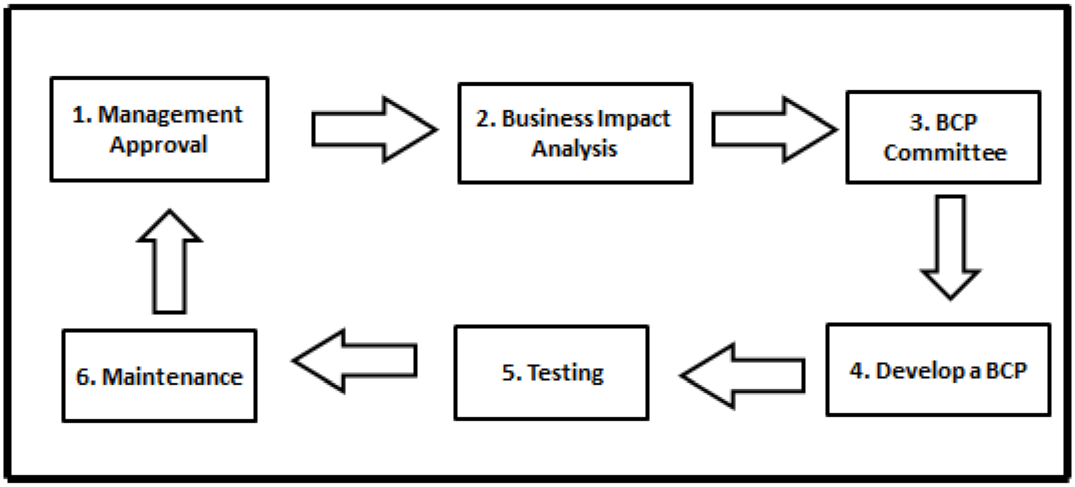

Figure 2: Common BCP Process (Cerullo and Cerullo, 2004; Botha and Von Solms, 2004)

However, the BCP lifecycle procedural process as proposed by British standard is shown below in Figure 3. This means the BCP process must be attained within such given lifecycle.

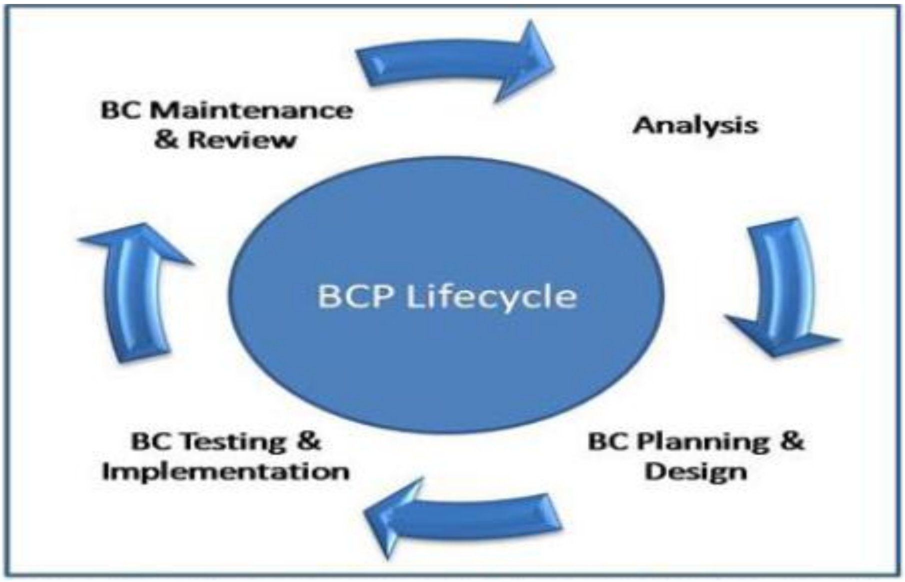

Figure 3: BCP Lifecycle (British Standard for BCP) (Al-Zahrani, 2010)

4. RESEARCH FOCUS

The majority of the information regarding BCP usually focuses on the development of continuity plans for large organizations thereby omitting the differences that existed when compared with smaller organizations. This research is an attempt to fill this gap by focusing on BCP strategies for SMEs especially in South Africa. The research adopted the case study approach within the qualitative research method.

Four organizations from Cape Town in South Africa which each had BCP in place and had prolonged downtime during a disaster were selected. The risk manager from each company was interviewed and the conversations 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).

The data from the four organizations that were being researched was analysed and summarized in a table format to obtain cohesion from the responses of each company and to establish a pattern as to why each company experienced prolong downtime during a disaster event. It thus become evident that certain aspect within their BCP has been overlooked and could not be implemented, thereby causing them to have prolonged downtime during a disaster.

Research Scenario and Methodology

The focus of this study is to understand the reason why organization that have BCP in place and implement consistent testing still experience prolong downtime during a disaster event. The research employed a face-to-face interviews and semi-structured questionnaire to keep the interviewer and interviewee focused and aligned with the research questions and objectives. Each interview was between 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 from each of the four organizations, who each had BCP in place, but still experienced prolong downtime during a disaster event were interviewed. The responses for each organization were recorded and interpreted using rapid miner software. Therefore, the research employed a two phased –data analytics method. First, the study explores descriptive analytics using a qualitative case study to provide insight into the past event. Second, the research provides a normative process model for BCP through prescriptive process (data mining of language processing). The reasons for these process is that it is most complicating that organizations cannot predict with any degree of precision the potential event of Infrastructure failure (Boin and McConnel, 2007). The case studies of the organizations with their respective responses are presented in Appendix A.

5. CONCEPTUALIZATION OF BCP PROCESSES

The research follow a simple research procedure by focusing on emerging concepts derived from the literature using content analysis to identify the causes of prolong downtime during a disaster event in South Africa SMEs. The occurring themes are as follows BCP, BCP process and Critical Success Factors. These three themes form the basis of this study and are expanded and conceptualized as follows:

- BCP: This highlights the Benefits, Challenges and Components of the ICT systems
- BCP Process: This identify various BCP processes in ICT system as represented in Figure 2
- Critical Success Factors – This covers factors that ensure BCP success and factors that lead to BCP failure.

The three theme are presented in Figure 4 below

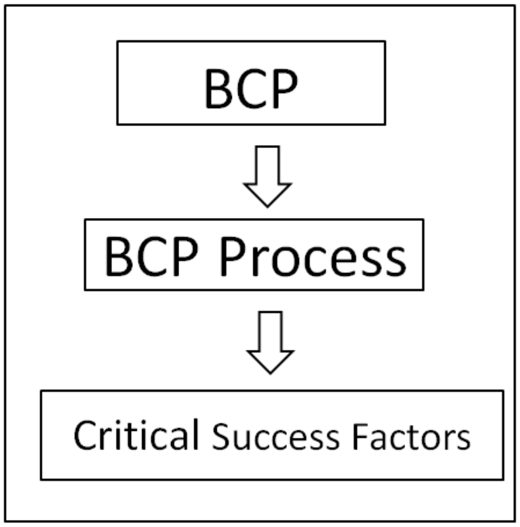

Figure 4: Conceptualized BCP common processes

The figure above shows the conceptual BCP common processes that are employed as the basis for the research.

6. DATA ANALYSIS AND RESULTS

As mentioned previously each organization that were chosen for this research had a BCP in place but still experienced prolongs downtime during a disaster. The study refers to these four organizations as Company A to D for the purpose of confidentiality.

Using the above BCP common processes, data were analysed for Company A to D based on the responses obtained from Risk managers/BCP managers and other staffs from each of the four organizations (Company A to D) (see Appendix A for the Cases). The table below is a summary of the primary reasons for the prolonged downtime during their respective disaster experienced by each of the four organizations companies that were researched.

Table 1: Reasons for the prolonged downtime per company

Companies	**Summary of reasons for failure**
Company A	We took the supply of electricity for granted and therefor never included it into our BCP.
Company B	We **overlooked** to include the routers in our BCP and therefore it was never tested.
Company C	We **overlooked** to fully monitor all critical elements within an application, therefore weren't able to provide proper support in the event of a failure.
Company D	We failed to identify redundancy for that connection or **overlooked** that network connection.

If the reader observe the responses for each organization (named Company A to D) as summarised in the above Table 1, there is a commonality in that most of the organizations (company B to D) overlooked hardware peripherals such as routers, network connection and as well as software peripheral which is the ICT service responsible for allowing an application to operate. This led to new BCP procedural process and presented in Figure 4 below

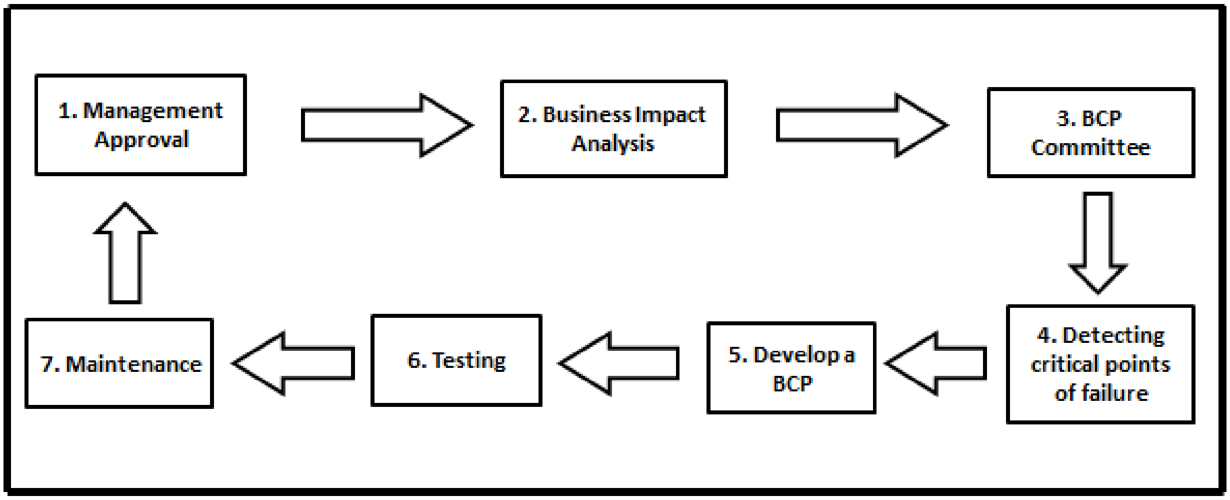

Figure 4: Proposed normative BCP process model.

Following the research conducted within the four organizations based in Cape Town, South Africa, it is evident that there is a vital gap within their BCP Process. The reader would observe that the BCP process model in Figure 1 when compared with Figure 4, it is apparent that an additional step has been added. To iterate on the point 4 “Detecting critical points of failure” the following should be documented under this point. Therefore the following procedure should be ensured

(i) 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 and as well as the technical manager.

(ii) Identify, test and signoff each point of failure based on the architectural diagram.

(iii) Rank and rate each point of failure, so that only significant points of failure are incorporated into the final BCP document.

After these iterative periods, the future analysis could employ the predictive modelling for further decisions in the process model.

7. CONCLUSION

The major aim of this research is to determine why companies that have BCP in place still experience prolonged downtime during disaster period based on systems integrations, most organizations have realized that their business are now more dependent on ICT than ever before and that greater focus should be placed on BCP to ensure that organization do not experience prolong downtime during a disaster. It is therefore imperative that organizations should strengthen their BCP and close any loop holes that might exist therein by looking critically into certain elements or criteria area causing prolong downtime during a disaster. Therefore organizations adopting the BCP Process as stated in the normative BCP process model should incorporate the missing steps / criteria so as to minimise downtime during any disaster period.

The present research has several implications: First, given that limited scholarly literature regarding BCP in SMEs existed, this study contributes to the body of knowledge in this regard.

Second, the theoretical normative BCP process model proposed in the present study serves as a response to the call by the United Nation in the Sendai Framework (Disaster Risk Reduction: 2015-2030) for BCP model for SMEs especially in African countries. Third, the study present both descriptive and prescriptive data analytics process for normative model formulation.

ACKNOWLEDGEMENT

This research project from which this work derives was part of the Masters research of the Second Author under the supervision of the First Author at the University of the Western Cape, South Africa in 2013.

The First Author improved the research significantly through methodology, framework and wrote the entire document.

The research also benefited from grants from National Research Foundation (NRF) Fund through the Incentive Fund for Rated Researcher Scheme.

REFERENCES

Al-Zahrani, A (2010) "Decision making assessment model throughout IT Business Continuity Planning (BCP) Lifecycle in small or medium-size organizations in Saudi Arabia" Open University Malaysia.

Boin, A., & McConnel., A. (2007). Preparing for Critical Infrastructure Breakdowns: The "A The Limit of Crisis and the Need for Resilience. *Journal of Contingencies and Crisis Management. Vol 15(11), 1-59.*

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

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.

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

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

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

Karakasidis, K. (1997). "A project planning process for Business Continuity." KPMG Information Technology Consulting Division, Melbourne, Australia

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

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

Moore, P (1995) "Critical elements of a disaster recovery and business / service continuity plan" Volume 13 Pages 22 – 27

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

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

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, 1-15.

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

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

United Nation (2015). Sendai Framework for Disaster Risk Reduction 2015-3020. http://www.unisdr.org/we/coordinate/sendai-framework.

Appendix A

Finding of Case Study 1 (Company A)

Company A

Company A is one of South Africa's largest outdoor retail stores, with more than a 100 branches all over South Africa as well as in Namibia and Botswana. The organization is well established and reputable SME in South Africa's retail market. The company employs about 1000 to 1500 permanent and casual staff nationally. There are about 500 permanent employees at their Head Office. Each branch is equipped with the latest computer terminals on which the Point of Sale (POS) software is installed. These computer terminals are connected to the back office terminal which is situated in the store manager's office. The back office terminal for each store constantly communicate with the servers at Head Office to report back sales transactions, stock levels of each item, credit card transactions. If a server "goes down" meaning that either the server crashed or the network lines between a store and the Head Office is not operational, that store is "shut out" from the outside world and has to trade manually. This means that staff members within the store has to write down each cash transactions in an invoice book. No debit or credit cards 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.

Disaster of Company A

On the 20th 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 last for 10 minutes thereby allowing the system administrator to gracefully shutdown all servers. All servers, network switches, routers and other electronic equipment that uses 220 VAC power is now non-operational. Communication between all stores and Head Office was down, thereby causing stores to be "shut out", meaning that the above scenario comes into play.

The impact of this disaster on business was as follow:
All stores had to trade manually and turn away customers that want 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 were 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 will never experience a power failure seeing that the company is on the same power substation as parliament. The company had therefor made no provisions or alternatives for the event of a power failure. This decision has proved to be catastrophic. As previously stated a disaster of this magnitude can definitely cause both financial and reputable damage.

A summary of the questions answered by the Risk Manager is in the table below

Table 11: 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 11 above is an indication that the company took the power factor for granted, even though in power failures are one of the most common disaster that a company can experience.

The table below is an analysis of the answers to the questions that relates to the key elements of an effective BCP

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 2.7
2	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	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	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	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	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	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	It was agreed by auditing committee that there is a recovery window for BC purposes.	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 & 15 in the table above is an indication that Company A conformed to some of the key elements of an effective BCP.

Findings of Case Study 2 (Company B)

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 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.

Their corporate clients comprise of blue-chip corporations, listed and non-listed entities and multi-nationals.

Their institutional clients are fund managers – large and small, traditional and alternative.

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 profile. 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.
Client has 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 profile 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.

Disaster of Company B

The company has a web portal that allows all clients to check the status of their investments and also allowing 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 the DR site. The primary router connects the entire company both locally and internationally to each other and to its clients. If for some reason the 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 failover 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 was not met. The company's reputation was also damaged.

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

: 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 the table 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.

The table below is an analysis of the answers to the questions that relates to the key elements of an effective BCP n

Analysis of Company B’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	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	Yes	Get senior management involved and keep them committed.
6	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.	In order for a plan to succeed, there must be multiple agency cooperation and involvement.
8	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	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	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	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 of questions 2, 5, 6, 8, 9, 13 and 15 in the above table, it highlight that most of the key elements of a BCP had been adhere to by Company B.

Findings of Case Study 3 (Company C)

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 are currently listed on the JSE. Even though their Head Office 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.

Disaster of Company C

On Saturday the 25 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 and would every time reboot the system with the hope that the system would reset itself. The phones in the service desk rang all day from frustrated vendors as most of their patrons would walk out of the store thereby causing them to lose revenue. After half the day has passed, the service desk operator then 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 that an email be sent to the appropriate parties concerned.

The interview with the Risk Manager revealed that monitoring the services of the applications has been overlooked, and therefore was not listed in the BCP strategy document 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 has they could not access the main server. This certainly had a great financial impact on the company and also damaged there reputation.

The table below is a summary of the answers given by the Risk Manager for company C.

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(bolded) in the above table is proof that not only should the software be monitored, but also the application as well as services of any application.

The table below is an analysis of the answers to the questions that relates to the key elements of an effective BCP

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	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	Yes, there is a Business Continuity Management (BCM) team that looks after enterprise wide BCP.	Get senior management involved and keep them committed.
6	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	Every 6 months. Real time replication, that allows all new applications to be included automatically. Some critical applications are reviewed quarterly.	Keep the plan current – Update the plan as applications gets updated
9	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	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	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 the table above it highlights that most of the key elements of a BCP had been adhere to by Company C.

Findings Case Study 4 (Company D)

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 and beyond. 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. The slightest mishap can be devastating and other similar companies will rejoice at this and use it to gain market share.

Disaster of Company D

On 16th 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 clients weren't able to surf the net, check emails, perform online banking, download, and so on, whilst businesses weren't able to do the same as the private clients, they weren't also unable 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 there 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 that the impact of the disaster certainly had a negative effect on the company's reputation as well as financial impact as many businesses had SLA's in place with their clients.

The table below is a summary of the answers of the BCP and Risk manager.

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 the table 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 which is relevant to their daily operations and that of their clients.

The table below is an analysis of the answers to the questions that relates to the key elements of an effective BCP as shown in

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 2.7**
2	"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	"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	"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".	In order for a plan to succeed, there must be multiple agency cooperation and involvement.
8	"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	"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	“Some applications are tested quarterly. Tests are performed on a departmental basis”.	Test the business recovery process and evaluate test results
15	“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.