International Journal of Electrical and Computer Engineering (IJECE)
Vol. 6, No. 5, October 2016, pp. 2425~2431
ISSN: 2088-8708, DOI: 10.11591/ijece.v6i5.11461

A Normative Process Model for ICT Business Continuity Plan for Disaster Management in Small, Medium and Large Enterprises

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

Article Info

Article history:

Received Apr 24, 2016
Revised Jun 29, 2016
Accepted Jul 15, 2016

Keyword:

Business continuity plan
Business process
Computer information systems
Data engineering & analytics
ICT service processes
Innovation
Risk management

ABSTRACT

Small, Medium and Large Enterprises (SMLs) are exposed 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 organizations. The current study offer both theoretical and practical implications for BCP in small, medium and large enterprises.

Corresponding Author:

Felix Olu Bankole,
School of Computing,
University of South Africa,
South Africa.
Email: olu.bankole@gmail.com

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 [1],[2]. 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 [3],[4].

Individual organization is unique, and as such will have a distinctive BCP, irrespective of similarities within industries and variations in organizational landscape [4], 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 [5],[6]. It is also considered as a process that ensures that operations and services are uninterrupted for the end-users or customers in an organization [1],[7]. The risk of business interruption in Small, medium and large enterprises expand as organization depends on ICT infrastructure services, therefore comprehensive procedures for BCP plan that would mitigate interruption of the business systems are required [1],[8],[9].

Small, Medium and Large Enterprises (SMLs) are playing an ever-increasing role in innovation, poverty alleviation and socio-economic development [6]. 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 operation processes [6],[10].

The causes of business interruption in organizations are not mainly from natural disasters but are multifaceted such as human errors in the systems, power outages and malicious threats [4],[6]. For example, in the UK, there was Cyber extortion in which a distributed denial of service attack on online gaming companies occurred [11], in the US, the Worldpay experienced a denial of service attack as a result of generated e-mail [12], 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 [12]. 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 [7].

The development of BCP has been a critical problem for most organizations and little literature that focuses on BCP management existed [3]. Though, most organizations especially in South Africa 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 [13].

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 ICT services in Small, Medium to Large Enterprises (SMLs), 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 SMLs organization. The research question focus on the type of BCP service required for management of disaster in SMLs.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 [14]-[16]. Disasters occur for a number of reasons, both routine and dramatic, and BCP must address every aspect of these incidents [14]. 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, provide higher information value for enterprise and to ensure essential business impact [12],[17],[18].

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 [19],[20].

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 [3]. 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 [3]

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 [21]. 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) [22]. In circumstances, 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 [19], 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: [3],[4].

(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:

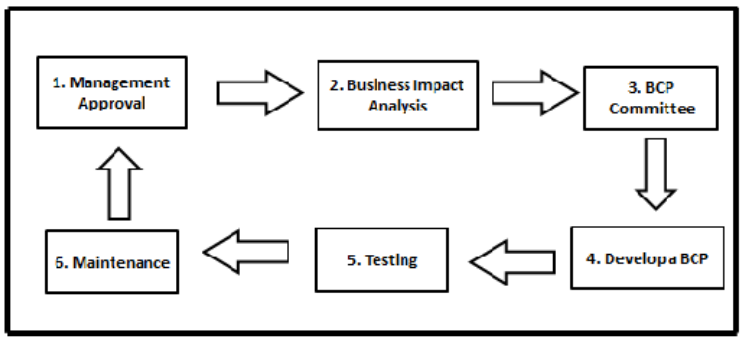

Figure 2. Common BCP Process [3],[4]

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.

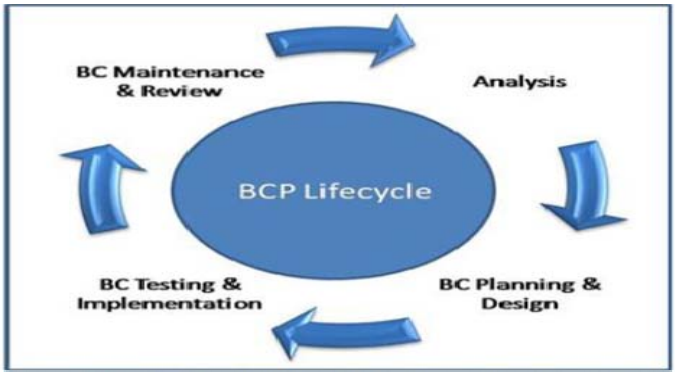

Figure 3. BCP Lifecycle (British Standard for BCP) [8]

4. RESEARCH FOCUS AND METHOD

The majority of the information regarding BCP usually focuses on the development of continuity plans for SMLs organizations thereby omitting the process plan that existed within the BCP lifecycle. This research is an attempt to fill this gap by focusing on BCP strategies for SMLs especially in developing and emerging economy such as 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 [23].

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.

4.1. 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) [8, 9]. 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 [9]. The case studies of the organizations with their respective responses are presented in Appendix A.

5. CONCEPTUALIZATION OF BCP PROCESS

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 SMLs. 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 themes are presented in Figure 4 below:

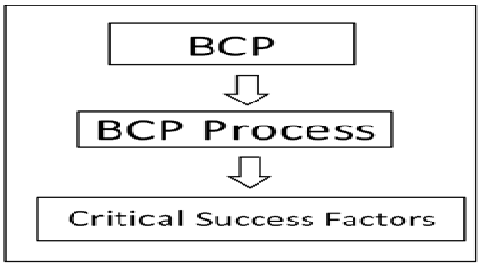

Figure 4. Conceptualized BCP common processes

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

6. DATA ANALAYSIS 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

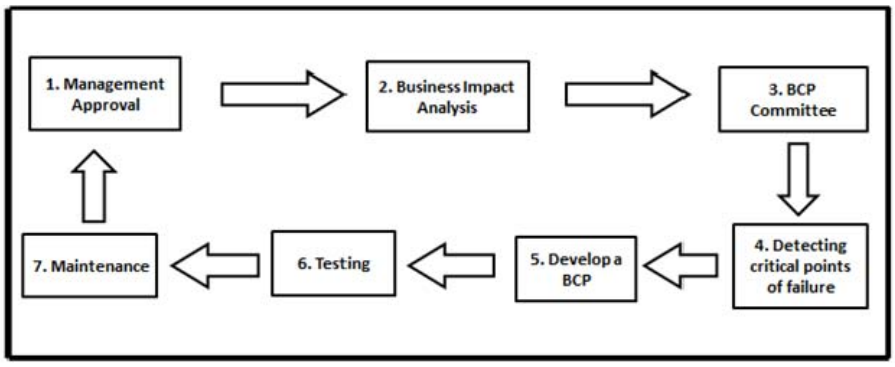

Figure 5. Proposed normative BCP process model

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 2 when compared with Figure 5, 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 procedures 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 avoid any incident 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 conceptualized 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 SMLs 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 SMLs in both developed and developing countries. Third, the study present both descriptive and prescriptive data analytics process for normative model formulation.

ACKNOWLEDGEMENTS

This research project from which this work derives was a part of the Masters research of the FIRST author under the mentoship (supervision) of the SECOND author at the University of the Western Cape, South Africa in 2013.

The earlier version of the work was presented as proceedings of United Kingdom Academy for Information Systems Conference (UKAIS), Oxford University. UK.

REFERENCES

[1] J. K. Akram, "Business Disaster Preparedness: An Empirical Study for Measuring the Factors of Business Continuity to face Business Disaster," *International Journal of Business and Social Science*, vol/issue: 2(18), pp. 183-191, 2011.
[2] P. Moore, "Critical Elements of a Disaster Recovery and Business," *Service Continuity Plan*, vol/issue: 13(1), pp. 17-17, 1995.
[3] A. Boin and A. McConnel, "Preparing for Critical Infrastructure Breakdowns: The Limit of Crisis and the Need for Resilience," *Journal of Contingencies and Crisis Management*, vol/issue: 15(11), pp. 1-59, 2007.
[4] J. Botha and R. V. Solms, "A Cyclic Approach to Business Continuity Planning," *Information Management & Computer Security*, vol/issue: 12(4), pp. 328-337, 2004.
[5] L. Harris, "Keeping IT Alive when Disaster Strikes," 2001. Retrieved on 2011-08-12 from http://www.itweb.co.za/index.php?option=com_content&view=article&id=44662&catid=116.
[6] N. Phelps, "Setting up a Crisis Recovery Plan," *The Journal of Business Strategy*, 1986.
[7] N. Altay and G. G. Walter, "Interfaces with other Disciplines: Preparing. OR/MS Research in Disaster Operations Management," *European Journal of Operational Research*, vol/issue: 75(1), pp. 475-493, 2006.
[8] A. A. Zahrani, "Decision Making Assessment Model throughout IT Business. Continuity Planning (BCP) Lifecycle in Small or Medium-size Organizations in Saudi Arabia," Open University Malaysia, 2010.
[9] O. J. Ayangbekun, *et al.*, "Analysis of Security Mechanisms in Nigeria E-Banking Platform," *International Journal of Electrical & Computer Engineering*, vol/issue: 4(6), pp. 837-847, 2014.
[10] M. Swanson, *et al.*, "Contingency Planning Guide for Federal Information Systems," Nist Special Publication 800 – 34 Rev 1, 2010.

[11] C. Nickolette and J. Schmidt, "Business Continuity Planning – Description & Framework," Business Continuity Planning White paper, 2001.
[12] S. Fade, "Using Interpretative Phenomenological Analysis for Public Health Nutrition Dietetic Research: A Practical Guide," *Proceedings of the Nutrition Society*, vol. 63, pp. 647-653, 2004.
[13] R. Grimaldi, "Why do Business Continuity Plans fail?" *Journal Risk and Insurance*, 2002. Retrieved http://www.rmmag.com/Magazine/PrintTemplate.cfm?AID=1483.
[14] V. Cerrulo and J. M. Cerrulo, "Business Continuity Planning: A Comprehensive Approach," *Information Systems Management*, vol/issue: 12(1), pp. 70-78, 2004.
[15] H. F. Cervone, "Managing Digital Libraries: the view from 30,000 feet. Disaster Recovery and Continuity Planning for Digital Library Systems," *OCLC. Systems & Services*, vol/issue: 22(3), pp. 173-178, 2006.
[16] M. Croy and J. E. Geis, "Acronym soup: BCP, DR, EBR—what does it all mean?" *Disaster Recovery Journal*, vol/issue: 18(3), 2005.
[17] F. Gibb and S. Buchanan, "A Framework for Business Continuity Management," *International Journal of Information Management*, vol/issue: 26(1), pp. 128-141, 2006.
[18] A. Albarda, "Characteristics in Classsification of Information Use," *International Journal of Informatics and Communication Technology*, vol/issue: 3(3), 2014.
[19] Insurance Information Institute, "Prepared for the Worst? Small Businesses gets help for Disaster," 2010.
[20] K. Karakasidis, "A Project Planning Process for Business Continuity," *KPMG Information Technology Consulting Division, Melbourne, Australia*, 1997.
[21] A. Kirschenbaum, "The Missing Link in Business Continuity," *Disaster Recovery Journal*, vol/issue: 19(4), pp. 54-55, 2006.
[22] Sayen Organisation, "Understanding Disasters," *Internship Series*, vol. 3, 2008. Available http://www.sayen.org/Volume-III.pdf.
[23] Y. D. Daniel, "Business Continuity Planning: An Empirical Study of Factors That Hinder Effective Disaster Preparedness of Businesses," *Journal of Economics and Sustainable Development*, vol/issue: 5(27), pp. 185-191, 2014.