

**KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**KUMASI**

**INSTITUTE OF DISTANCE LEARNING**



**BUSINESS CONTINUITY FOR FINANCIAL INSTITUTIONS  
A CASE STUDY OF SG-SSB LIMITED**

**BY**

**DANIEL KOFI ANTWI, BSC. BUILDING TECHNOLOGY**

**A DISSERTATION SUBMITTED TO THE INSTITUTE OF DISTANCE  
LEARNING, KWAME NKRUMAH UNIVERSITY OF SCIENCE AND  
TECHNOLOGY IN PARTIAL FULFILMENT OF THE REQUIREMENTS  
FOR THE AWARD OF DEGREE OF**

**COMMONWEALTH EXECUTIVE MASTERS OF BUSINESS  
ADMINISTRATION.**

**JUNE 2011**

## DECLARATION

I hereby declare that this submission is my own work towards the CEMBA and that to the best of my knowledge, it contains no material previously published by another person nor material which has been accepted for the award of any other degree of the University, except where due acknowledgment has been made in the text.


**DANIEL KOFI ANTWI**  
**PG3039109**

.....  
Signature

.....  
Date

Certified by Supervisor:

**DR. EMMANUEL ADINYIRA**  
Department of Building Technology  
KNUST  
Kumasi-Ghana

  
.....  
Signature

14/09/2011  
.....  
Date

Certified by:

**PROF. ISAAC KWAME DONTWI**  
**Dean Institute of Distance Learning**  
KNUST  
Kumasi-Ghana

.....  
Signature

.....  
Date

## **Dedication**

To my Lord and Savoir Jesus, my late mother Mad. Ama Adoma, may her soul rest in eternal peace and my unborn children.

# KNUST



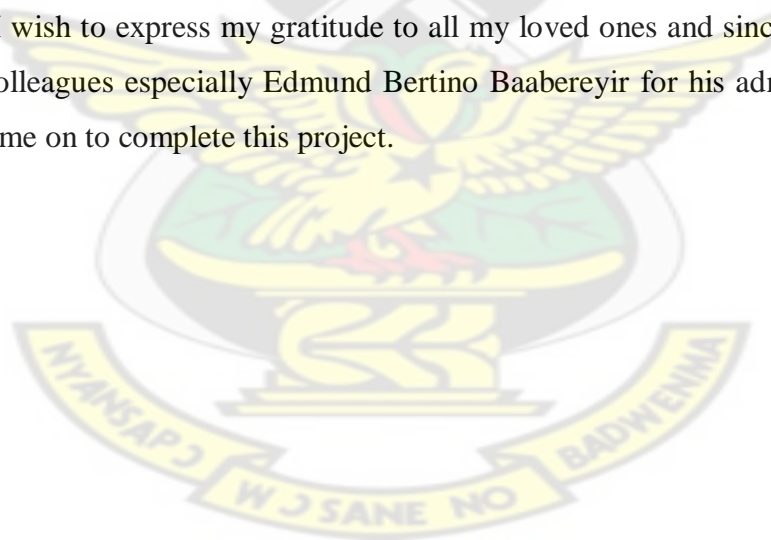
## **Acknowledgement**

This research work was not my singular effort because many people contributed either directly or indirectly. I therefore wish to extend my gratitude to those individuals who supported and motivated me. I give glory and honor to my Lord and Saviour Jesus Christ who has always been there for me when no one was.

Special thanks to my brothers for always having my back and thanks to my sweetheart, friend and intercessor.

With not many words to express my sincere appreciation, am very grateful to my friend and supervisor Dr. Emmanuel Adinyira whose wise counsel, corrections, constructive criticisms and most of all inspiration have been of great help to me. My sincere thanks to my course and group mates Atsu Freeman, Abigail Allotey and Priscilla Cofie for the discussions, ideas and friendship we shared and continue to share together. Not forgetting my former bosses Mr Kwame Aboagye and Mr Douglas Frimpong, whose counsel and mentoring have brought me this far.

Lastly, I wish to express my gratitude to all my loved ones and sincere thanks to my office colleagues especially Edmund Bertino Baabereyir for his admonishing which spurred me on to complete this project.



## **Abstract**

Increasing competition in the financial sector, demands by customers for 24hr continuous service, increasing regulatory or policy requirements, and increasing threats have exerted pressure on financial institutions to develop comprehensive contingency plans that ensure the continuity of their business processes. A properly-designed, implemented and tested Business Continuity Plan (BCP) is the best insurance against financial peril for any financial institution or organisation in general.

The main aim of this project is to affirm the relevance of business continuity plan to financial institutions. It involved an investigation into the existence of such a plan, the major operational areas and scenarios the plan covers, stakeholders involved in the development of the plan, the training and understanding that stakeholders have on the plan and whether the plan is tested periodically. Société Générale Social Security Bank (SG-SSB) Limited was used as a case study. Data was collected via mailed questionnaire and oral interview with the BCP manager. 100 questionnaires were sent out and with a 69% response rate. Percentages, mean, variance and standard deviation were calculated from responses and inferences were drawn from them.

The research findings revealed that SG-SSB has a business continuity plan in place which covers its major operations based on specific scenarios or incidents. It was also revealed that the company's board of directors; senior Management; BCP manager; and staff were the main stakeholders involved in the development of the plan even though not every staff was involved. The company has programs and communication channels in place to train and inform staff so that they know their obligations and there is also a program to test the plan periodically in order to review and update it. All respondents affirmed the relevance of the BCP to financial

institutions and the BCP manager stressed on the priority the bank places on the plan not only in meeting its parent company's policies but for various reasons, pressures and demands in the financial industry.

# KNUST



<b>Table of Contents</b>	<b>Page</b>
Declaration.....	ii
Dedication.....	iii
Acknowledgement.....	iv
Abstract.....	v
Table of contents.....	vii
List of Table and Figures.....	x
Abbreviations.....	xi
<b>CHAPTER ONE.....</b>	<b>1</b>
<b>GENERAL INTRODUCTION.....</b>	<b>1</b>
1.1 RESEARCH BACKGROUND.....	1
1.2 STATEMENT OF PROBLEM.....	4
1.3 OBJECTIVES OF STUDY.....	5
1.3.1 Specific Objectives .....	6
1.4 RESEARCH QUESTIONS.....	6
1.5 SIGNIFICANCE OF THE STUDY.....	7
1.6 SCOPE OF THE STUDY.....	7
1.7 STRUCTURE OF THE THESIS.....	8
<b>CHAPTER TWO.....</b>	<b>10</b>
<b>LITERATURE REVIEW.....</b>	<b>10</b>
2.1 INTRODUCTION.....	10
2.2 THE EVOLUTION OF BCM.....	10
2.3 DEFINITIONS.....	15
2.3.1 Business Continuity .....	15
2.3.2 Business Continuity Planning.....	16
2.3.3 Business Continuity Management .....	16
2.4 HIGH LEVEL PRINCIPLES OF BUSINESS CONTINUITY.....	19
2.4.1 Principle 1: Board and senior management responsibility .....	22
2.4.2 Principle 2: Major operational disruptions .....	24
2.4.3 Principle 3: Recovery objectives .....	27
2.4.4 Principle 4: Communications.....	29
2.4.5 Principle 5: Cross-border communications .....	31
2.4.6 Principle 6: Testing.....	34
2.4.7 Principle 7: Business continuity management reviews by financial authorities .....	35
2.5 NEED FOR BCM.....	36
2.5.1 Rising competition and higher demands of customer .....	37
2.5.2 Increasing threat .....	37
2.5.3 Increasing supply and demand chain integratio .....	38
2.5.4 Increasing dependency on complex information system .....	38
2.5.5 Advent of process based approache .....	38
2.6 EFFECTIVE BUSINESS CONTINUITY MANAGEMENT .....	39



<b>CHAPTER THREE.....</b>	<b>41</b>
<b>METHODOLOGY.....</b>	<b>41</b>
3.1 INTRODUCTION.....	41
3.2 SG-SSB LIMITED AS THE CASE STUDY.....	41
3.2.1 Brief History of SG-SSB Limited.....	41
3.2.2 Corporate Mission of the Bank.....	42
3.2.3 Operational Risk and Permanent Control Department.....	42
3.2.4 Business Continuity Plan Manual for SG-SSB Limited.....	44
3.2.4.1 Policy.....	44
3.2.4.2 Recovery Overview.....	44
3.2.4.2.1 Recovery Objectives and Plan Scope.....	45
3.2.4.2.1.1 Objectives.....	45
3.2.4.2.1.2 Scope.....	45
3.2.4.2.2 Recovery Strategies.....	46
3.2.4.2.4.1 Banking BCP Strategy-Head Office.....	46
3.2.4.2.4.2 Banking BCP Strategy-Branch.....	46
3.2.4.2.4.3 IT BCP Strategy.....	47
3.2.4.2.3 Recovery Teams and Roles.....	47
3.2.4.2.3.1 Crisis Management Team.....	47
3.2.4.2.3.2 Incident Control Group.....	48
3.2.4.2.3.3 Business Unit Recovery Team.....	48
3.2.4.2.4 Recovery Procedures.....	49
3.2.4.3 Communication Procedures.....	50
3.2.4.4 Return to Normal Operations.....	50
3.2.4.4.1 Review of Events.....	51
3.2.4.5 BCP Testing and Review.....	51
3.2.4.5.1 Objective of Test.....	51
3.2.4.5.2 Test Strategy.....	52
3.2.4.6 Limitations.....	53
3.3 METHODOLOGY.....	53
3.3.1 Research Setting.....	53
3.3.2 Sources of Data.....	54
3.3.3 Study Population.....	54
3.3.4 Sample Size.....	54
3.3.5 Sampling Design and Technique.....	55
3.3.6 Measurement.....	55
3.3.7 Data Collection Methods.....	56
3.3.7.1 Questionnaire Design.....	56
3.3.7.2 Questionnaire Administration.....	56
3.3.8 Data Analysis.....	57
<b>CHAPTER FOUR.....</b>	<b>58</b>
<b>PRESENTATION AND ANALYSIS OF DATA.....</b>	<b>58</b>
4.1 INTRODUCTION.....	58
4.2 RESPONSES FROM BCP REPRESENTATIVES AND GENERAL STAFF (NON-BCP REPRESENTATIVES).....	58
4.2.1 Questionnaire Response Rate.....	58
4.2.2 Disruptions/Incidents in the Last 5 Years.....	59
4.2.3 Existence of Business Continuity Plan.....	59
4.2.4 Development of the Business Continuity Plan.....	60
4.2.5 Level of Training/Education on the BCP.....	61
4.2.6 Perceived Importance/Relevance of Business Continuity Plan.....	62
4.3 SUMMARY OF INTERVIEW AND RESPONSE FROM BCP MANAGER.....	63
4.3.1 Introduction.....	63
4.3.2 Existence, Development of BCP and Recovery from Disruptions.....	64
4.3.3 Training of Staff and Testing of BCP.....	65
4.3.4 Perceived Importance/Relevance of Business Continuity Plan.....	66



4.3.5 Perception of Threats.....	66
4.4 SUMMARY OF FINDINGS.....	69
<b>CHAPTER FIVE.....</b>	<b>71</b>
<b>DISCUSSIONS, CONCLUSION AND RECOMMENDATIONS.....</b>	<b>71</b>
5.1 INTRODUCTION.....	71
5.2 DISCUSSIONS.....	71
5.3 CONCLUSIONS.....	74
5.4 RECOMMENDATIONS.....	76
5.5 LIMITATIONS.....	77
5.6 FUTURE WORK.....	77
<b>Bibliography.....</b>	<b>79</b>
<b>Appendix A-Questionnaire.....</b>	<b>82</b>

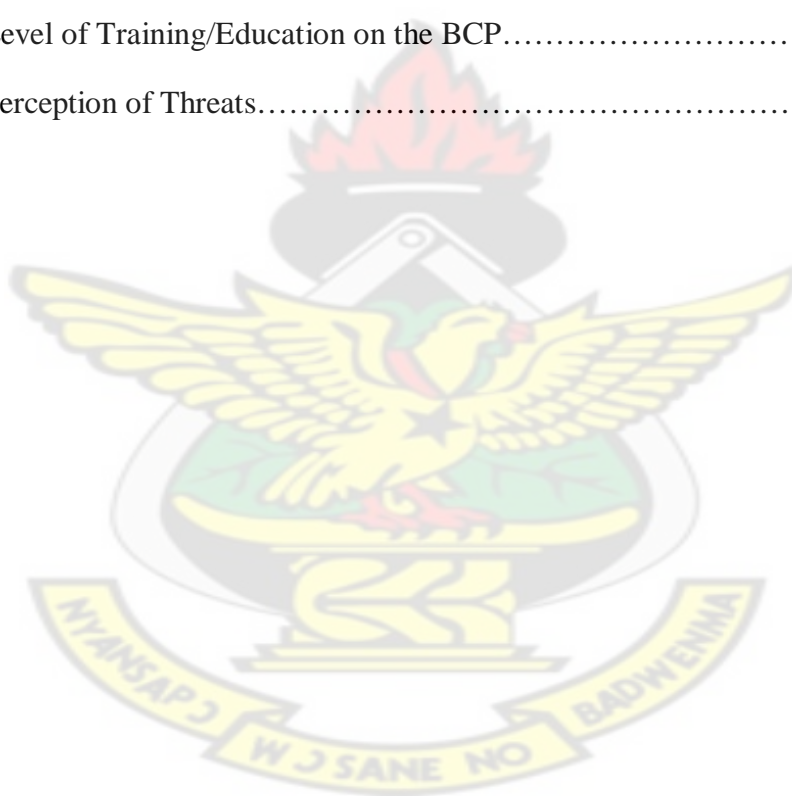


## List of Tables

4.1	Perceived Relevance of BCP.....	81
4.2	Perception of Threats.....	84

## List of Figures

4.1	Questionnaire Response Rate.....	75
4.2	Existence of BCP.....	76
4.3	Development of BCP.....	78
4.4	Level of Training/Education on the BCP.....	79
4.5	Perception of Threats.....	86



## Abbreviations

<b>ANSI</b>	American National Standards Institute
<b>BCBS</b>	Basel Committee on Banking Supervision
<b>BCM</b>	Business Continuity Management
<b>BCP</b>	Business Continuity Plan
<b>BHFM</b>	Banque hors de France (the International Retail Banking Division)
<b>BIA</b>	Business Impact Analysis
<b>BPI</b>	Business Process Improvement
<b>BPR</b>	Business Process Reengineering/Redesign
<b>BRCG</b>	Business Risk Consulting Group
<b>BURT</b>	Business Unit Recovery Team
<b>CCTA</b>	Central Computer and Telecommunication Agency
<b>FFIEC</b>	Federal Financial Institute Examination Council
<b>IAIS</b>	International Organisation of Securities Commissions
<b>ICG</b>	Incident Control Group
<b>IRTPA</b>	Intelligence Reform and Terrorism Prevention Act
<b>ISHN</b>	Industrial Safety and Hygiene News
<b>NFPA</b>	National Fire Protection Association
<b>NRP</b>	National Response Plan
<b>RPOs</b>	Recovery point objectives
<b>RTOs</b>	Recovery time objectives
<b>TQM</b>	Total Quality Management

## **CHAPTER ONE**

### **GENERAL INTRODUCTION**

#### **1.1 RESEARCH BACKGROUND**

Financial institutions could face the suspension of critical operations due to natural disasters, terrorist attacks, computer problems, and other causes and hence need to secure business continuity by formulating action plans in advance to ensure quick recovery.

Disasters can result in enormous losses – financial, investor confidence, and corporate image. It can also lead to serious legal issues, especially when more and more private data is being captured, stored, and transmitted across the very public internet. These losses and legal challenges can have a small, short-term impact but more often than not, they have a significant, long-term impact, and in some cases imperil the existence of the company (Snedaker, 2007).

Clearly Y2K and September 11, 2001 were the most significant wake-up calls for Business Continuity and Disaster Recovery Planning. The last few years have seen contingency planning progress from earlier issues of addressing primarily information services and data centre priorities, to include equally important corporate issues involving telecommunications, human resources, vital records, risk management, security, environmental concerns, product recovery, and the facility itself.

Financial institutions have a shared interest in promoting the resilience of the financial system to major operational disruptions. This interest is the result of multiple factors, including:

- The pivotal role that financial intermediation plays in facilitating and promoting national and global economic activity by providing the means for making and receiving payments, for borrowing and lending, for effecting transactions, for insuring risks, and for raising capital and promoting investment;
- Increasing complexity and operational risk across financial systems. Financial systems are keenly dependent on automation and, in turn, on those components of the physical infrastructure that support automation – such as telecommunications and power;
- The concentration of clearing and settlement processes in most financial systems. Disruptions of these processes can have material adverse consequences for a financial system and prevent significant market participants from completing transactions and meeting their obligations;
- Deepening interdependencies among financial industry participants within and across jurisdictions. The velocity with which money and securities turn over on a daily basis underpins the considerable interdependencies – in the form of settlement risk and, ultimately, credit and liquidity risks – among financial institutions and investors. The result is that operational disruptions at one financial institution can cause difficulties at others. Furthermore, given the increasing globalisation of markets, disruptions in one jurisdiction could have serious implications for others contagion effects;
- The possibility of terrorist or other malicious attacks targeted, directly or indirectly, at the infrastructure of the financial system;
- A strong interest in maintaining public confidence in financial systems. Repeated or prolonged interruptions to the operations of a financial system

undermine and could result in a withdrawal of capital from the system by domestic and global participants.

A well-designed, implemented and tested contingency plan is the best insurance against financial peril for any corporation, institution or organisation with a future (Moore, 1995). A bad plan or incomplete plan is often worse than no plan at all. An ill-conceived or incomplete plan may lead people to mistakenly assume that emergency and contingency plans are in place when, in fact they are not. A false sense of security can lead to an even bigger problem than the disaster event itself precipitates.

There is need for banks and financial institutions to have in place an effective Business Continuity Plan that will ensure their ability to operate on an ongoing basis and limit losses in the event of an operational disruption.

Business Continuity Plan has to be comprehensive in such a way as to include policies, strategies, plans, procedures and standards for ensuring that specified operations can be maintained or recovered in a timely manner in the event of a disruption and, by extension, ensures that the functionality of the financial system as a whole is preserved. One of the tangible evidence that an institution has embraced Business Continuity Management is the formulation of an effective and workable Business Continuity Plan (BCP).

A BCP sets out procedures, processes and systems necessary to continue or restore the operation of an organization in the event of a disruption. It provides detailed guidance for implementing the recovery plan and outlines the roles, responsibilities and succession in managing operational disruptions. It also defines triggers for activating the BCP and establishes business resumption teams for core business



processes. The resilience of a financial system to major operational disruptions will be determined by the robustness of the BCPs of all participants within the system.

## **1.2 STATEMENT OF PROBLEM**

Banks and financial institutions are susceptible to operational disruptions caused by internal and external threats such as fire, earthquakes, wars, terrorist attacks, system failures, etc. Such disasters may lead to severe operational disruptions and sometimes threaten the solvency and business continuity of institutions, which could adversely impact the financial system as a whole. In today's world, Business Continuity Management (BCM) is becoming increasingly important.

In a study of companies that experienced a major data loss without having solid Business Continuity/Disaster Recovery plan in place, 43% never reopen, 51% will close within two years, and only 6% will survive long-term (Cummings *et al*, 2005). That is a 94% mortality rate for companies that experience a major data loss. In August 2002, the American Management Association released a study indicating that more than half of the surveyed companies had no disaster recovery or crisis management plan in place. Another report from Gartner, Inc. in 2002, indicated that less than 10% of small and medium businesses had disaster plans, and that 40% of companies that experience a disaster without a disaster recovery plan will go out of business within five years. Looking specifically at fires, the most common disasters businesses experience, it is estimated that 44% of companies whose premises experience a significant fire do not recover at all, primarily because they have no Business Continuity/Disaster Recovery plans in place (Snedaker, 2007).

Snedaker (2007:7) mentioned that the World Trade Centre bombing in Manhattan in 1993 resulted in 150 out the 350 business located in the centre going out of business



– that is about a 42% failure rate. Contrast that with many of the financial firms who had well developed and tested Business Continuity/Disaster Recovery plans that were located in the Twin Towers on September 11, 2001 – majority of them were back up and running within days.

Business Continuity and Disaster recovery plans were certainly put to the test by many financial firms after the terrorist attacks in the United States on September 11, 2001; but even years later, there are many firms that still do not have any type of business continuity plan in place. It seems insane not to have such a plan in place, but statistics show that many financial institutions do not even have solid data backup plans in place. Given the enormous cost of failure, why are many companies behind the curve? This research work affirms the relevance of Business Continuity Planning to financial institutions and analyses the disaster preparedness of financial institutions to major disasters and disruptions by examining the Business Continuity Management policies, standards and practices of SG-SSB Limited, a major player in the Ghanaian financial sector. It goes further to test the awareness of staff and stakeholders of the existence of the plan and the understanding of their responsibilities should the plan be invoked.

### **1.3 OBJECTIVES OF STUDY**

The aim of the study is to affirm the relevance of Business Continuity Planning to financial institutions.

### **1.3.1 Specific Objectives**

To achieve the main objective, the study focussed on the following specific objectives:

- To find out whether SG-SSB Limited has a Business Continuity plan in place, whether the plan covers major operational activities and which specific scenarios or incidents were considered in preparing the plan.
- To find out whether the bank undertakes periodic testing of the plan to review and update the plan and whether there is a periodic training of staff so that they know about the plan and their responsibilities.
- To determine the involvement of management, various heads and staff in the formulation of the BCP.
- To test the awareness of staff of the existing BCP.
- To evaluate the understanding of staff of their responsibilities if the plan is invoked in the event of a disruption.

### **1.4 RESEARCH QUESTIONS**

The research addresses the following research questions;

- Does SG-SSB Limited have a Business Continuity Plan in place and what operational activities does it cover?
- Does SG-SSB Limited test the plan periodically and train staff periodically?
- Who were the main stakeholders involved in the formulation of the plan?

- Are staff aware of and familiar with the existing business continuity plan?
- Do staff understand their obligations in the event the plan is invoked, and are they comfortable with their level of training and preparation?

## **1.7 SIGNIFICANCE OF THE STUDY**

The research is relevant in its portrayal of the following;

- A well-designed, implemented and tested business continuity plan is the best insurance against financial peril for any corporation, institution or organisation with a future. A bad plan or incomplete plan is often worse than no plan at all.
- A comprehensive BCP guides banks and financial institutions in making adequate preparations to deal with possible business interruption scenarios.
- The involvement of Board of Directors, Management, Head of Departments and staff in the formulation of a comprehensive BCP is critical to ensure the continuous delivery of relevant services to customers. Failure to do so may result in loss of banking licence; confidence; business and customers; cash flow; efficiency; financial and/ or management control; management visibility; and reputation.

## **1.8 SCOPE OF THE STUDY**

The study was limited to only SG-SSB Limited, interviews were conducted and questionnaires administered to key managers and staff of the bank. SG-SSB was selected because it is a major player in the banking industry and its respect for

procedures and banking regulations serves as benchmark for players in the banking industry.

## **1.9 STRUCTURE OF THE THESIS**

The thesis is presented in five chapters as follows: Chapter One constitutes the introduction of the study. This includes: the background, objectives and significance of the study. It also specifies the scope of the study.

Chapter Two reviews literatures on Business Continuity Planning. For this purpose several definitions for BCP are presented. The chapter also explains the need for BCP and define terminologies used in Business Continuity Management. This is to make the reader appreciate the relevance of the current research especially in the Ghanaian context. It further helps to deepen the entire conception of the thesis and provide a specific context for the study.

Chapter Three gives a history of the SG-SSB Limited, which is the main focus of the study; its corporate mission and scope of activities. It highlights the Business Continuity Planning policies, standards and practices of the bank. The chapter also talks about the research methodology comprising the sources of data, data analysis and presentation, sampling design and technique. It also details out the methods of data collection and analysis: the questionnaire design, questionnaire administration and difficulties.

Chapter Four presents the data and analysis of the data from the field work. It also carries a summary of the main findings of the study.

Chapter Five presents the discussions which relate research findings with the theories, conclusions which are researcher's opinions from findings as per the objectives of the study, recommendations which are the way forward resulting from the conclusions. The chapter also details out the limitations of the study and gives areas for future research.

# KNUST



## CHAPTER TWO

### LITERATURE REVIEW

#### 2.1 INTRODUCTION

This chapter gives the evolution of Business Continuity Management/Planning and reviews various literatures on the Business Continuity Management subject, the evolution of Business Continuity Management (BCM), various definitions of BCM/BCP, high level principles of BCP and the need for BCM by financial institutions. Finally, the chapter ends with the key processes involved in BCM/BCP.

#### 2.2 THE EVOLUTION OF BCM

Business Continuity Management, as a recognized business program, has evolved over the past twenty plus years from a technology centric disaster recovery function dealing almost exclusively with data protection and recovery to a much wider holistic and enterprise wide supporting focus (Wheatman *et al.*, 2001). Despite some strides to evolve BCM into a profession including a widely accepted common body of knowledge and terminology, standards of performance, and certification process, progress has been slow and is hampered by the fact that BCM, though generally recognized as a strategic function, remains a discretionary program for all but the most highly regulated business sectors such as the financial sector and healthcare sector. Even within these regulated sectors, standards of performance for all BCM supporting functions may not be recognized and specified in sufficient detail to ensure a truly comprehensive and integrated program.

As Mitroff (1992) concludes from his extensive research in the area of business crisis management (his umbrella term for an integrated BCM program), most businesses do



not have an adequate crisis management program, supported by corporate culture, individual and organizational level expertise, infrastructure and plans and procedures to fully understand, prepare for, and manage the crises they may face. Mitroff has since updated his conclusions in the 2001 book, *Managing Crises Before they happen* where he states that “The vast majority of organizations and institutions have not been designed to anticipate crises or to manage them effectively once they have occurred. Neither the mechanics nor the basic skills are in place for effective crisis management (Mitroff, 2001)”.

His conclusions are further supported by the results of the 2001 Business Continuity Readiness Survey, jointly conducted by Gartner, Inc. Executive Programs and the Society for Information Management that found “Less than 25 percent of Global 2000 enterprises have invested in comprehensive business continuity planning (Gartner, 2002)”.

This trend in BCM acceptance is changing, however. The reality of business is that increasing and dynamic natural, technological and human induced threats, business complexity, government regulation, corporate governance requirements, and media and public scrutiny demand a comprehensive and integrated approach to business crisis and continuity management. Classic natural, technological and human induced events such as Hurricane Andrew (1992), the Northridge Earthquake (1994), the Exxon Valdez oil spill (1989), the Bhopal chemical release (1984), the World Trade Center attack of 1993, and the Tylenol poisoning case (1982) have provided lessons learned that emphasize each of these factors and the need for coordination and cooperation within and between organizations, and between all levels of government, the private and not-for-profit sectors.



These lessons have not been lost by many businesses that have reached the conclusion that integrated BCM should be viewed as an investment rather than an additional cost that detracts from profits and have implemented their vision of comprehensive programs. The United States Business Roundtable, an association of business chief executive officers of leading corporations with the stated objective of improving public policy, explicitly recognizes the role of the Board of Directors and Management in the area of corporate governance in general, including specific business crisis and continuity management responsibilities. The Roundtable's white paper *Principles of Corporate Governance* charges the Board of Directors to periodically review management's plans for business resiliency and designate management level responsibility for business resiliency. Within the scope of business resiliency various functions are specifically mentioned and include business risk assessment and management, business continuity, physical and cyber security, and emergency communications (The Business Roundtable, 2002). However, lacking recognized standards and incentives, many businesses still consider BCM as a burdensome cost that receives minimal or even no support.

The tragic events of September 11th, 2001 and the implications for businesses directly and indirectly impacted by the events have further reinforced the need for enterprise wide coordination of the multiple functions supporting business crisis and continuity management. Studies following the attacks of September 11th, 2001, such as the 9/11 Commission study and report have engaged the United States government, at all levels, in the process of recognizing the responsibilities of the private sector and encouraging the private sector to take adequate steps to protect people, property and business operations. Further steps, including mandated

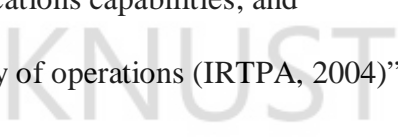
standards, may well follow beyond the current level of encouragement and voluntary compliance.

With roughly 80% of America's critical infrastructure managed by the private sector (The Conference Board, 2003), The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* recognizes that the "private sector generally remains the first line of defence for its own facilities," and encourages private sector owners and operators to "reassess and adjust their planning, assurance and investment programs to better accommodate the increased risk presented by deliberate acts of violence (The National Strategy, 2003)". The most recent versions of the *National Response Plan* (January 2005) and the *National Incident Management System* (March 2004) include the private sector in all phases of crisis and emergency awareness, prevention, preparedness, response and recovery planning and operations. The *National Response Plan* explicitly charges the private sector to enhance overall readiness (NRP, 2005).

Supporting this goal of improved private sector readiness and intra and inter sector coordination, the 9/11 Commission chartered the American National Standards Institute (ANSI) to develop a consensus on a national standard for preparedness for the private sector (9/11 Commission 2004). Based upon its collaboration with the National Fire Protection Association (NFPA) and the research of the 9/11 Commission, the "American National Standards Institute (ANSI) recommended to the 9-11 Commission that the National Fire Protection Association Standard, NFPA 1600 *Standard on Disaster/Emergency Management and Business Continuity Programs*, be recognized as the national preparedness standard (ISHN, 2004)". The

9-11 Commission report contains the following recommendation concerning private sector emergency preparedness and business continuity:

“Preparedness in the private sector and public sector rescue, restart, and recovery of operations should include, as appropriate –

- (A) a plan for evacuation;
- (B) adequate communications capabilities; and
- (C) a plan for continuity of operations (IRTPA, 2004)”.

The Act goes on to state that the NFPA 1600 standard “establishes a common set of criteria and terminology,” and charges the Department of Homeland Security to “work with the private, as well as government entities (IRTPA, 2004)”. The Sense of Congress included in the Act falls short of mandating national standards for the private sector, but does encourage the adoption of voluntary standards such as those included in NFPA 1600.

The implications of the Act and the evolution of national standards on the private sector will certainly evolve over a period of time; however, there is already high level conjecture and discussions that compliance with NFPA 1600 will be established as an acceptable "legal standard of care" owed by businesses to their employees and the general public and will serve as a "safe harbour" to minimize potential legal liability. Compliance with NFPA 1600 may also find its way into insurance considerations including insurability, premium pricing, and deductible levels. Additionally, proof of adequate “preparedness” is increasingly finding its way into contractual agreements between the public and private sectors and between private

sector businesses. Such requirements gained prominence in the preparations for Y2K, but lacked any real standard to demonstrate compliance. NFPA 1600 standards, though voluntary, appear to be the foundation of widely accepted national standards. Legal protection, insurance savings and contract requirements are certainly incentives for “preparedness” for all businesses and may be supplemented by additional measures such as tax savings and other forms of preferential treatment for business to business and business to government interactions.

## **2.3 DEFINITIONS**

### **2.3.1 Business Continuity**

“A pro-active process which identifies the key functions of an organisation and the likely threats to those functions” (British Standards, 2008a).

“A progression of disaster recovery, aimed at allowing an organisation to continue functioning after (and ideally, during) a disaster, rather than simply being able to recovery after a disaster” (Wikipedia, 2008b).

“An ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies, recovery plans, and continuity of services” (NFPA 1600, 2007:1600-4).

### **2.3.2 Business Continuity Planning**

“The advance planning and preparations that are necessary to identify the impact of potential losses; to formulate and implement viable recovery strategies; to develop recovery plan(s) which ensure continuity of organisational services in the event of an event/incident/crisis; and to deliver a comprehensive training, testing and maintenance programme” (BCI, 2008).

“The advance planning and preparations which are necessary to identify the impact of potential losses; to formulate and implement viable recovery strategies; to develop recovery plan(s) which ensure continuity of organisational services in the event of an emergency or disaster; and to administer a comprehensive training, testing and maintenance programme” (British Standards, 2008a).

Eric Jones, assistant vice president and manager, BRCG’s U.S. operations defines business continuity planning as

“Business continuity planning, or a BCP, is just one element of business continuity management. A BCP is drawn from information-gathering and risk assessments, and involves assigning responsibilities to key individuals, who then create recovery strategies based on specific objectives” (Reason Magazine, March 2007, p. 18)

### **2.3.3 Business Continuity Management**

The term Business Continuity Management was introduced for the first time in the end of the 1990's. However, BCM has only recently started to gain substantial momentum within organizations. Recent incidents like the Y2K threat (Oud, 2000),

(Koch, 2001) and the event on 9/11 (Yankee Group, 2001) have made an important contribution in this rise of awareness.

A proper definition of the concept is a prerequisite to define the scope of this study. The CCTA (1995-1) states that 'BCM is concerned with managing the risks to ensure that at all times an organization can continue operating to, at least, a predetermined minimum level'.

The Business Continuity Institute defines BCM as:

'A holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.' BS 25999, the British Standard for BCM, provides a basis for understanding, developing and implementing BCM within an organisation.

Spring Singapore (2005) uses the following definition: 'BCM is a holistic management process of identifying potential incidents that threaten an organization and the development of plans to respond to such incidents. It covers a broad spectrum of business and management disciplines, including risk management, disaster recovery and crisis management.'

FM Global uses the Business Continuity Institute's definition but Stuart Selden, assistant vice president and manager, FM Global's Business Risk Consulting Group (BRCG) further defines BCM as "A business culture rather than a project – a continual effort by all members of an organisation to help build resilient processes.



It's a framework that combines various elements of risk management and related disciplines, which can ultimately lead to an action oriented document called the business continuity plan, or BCP" (Reason Magazine, March 2007, p.18).

"Business continuity management provides the availability of processes and resources in order to ensure the continued achievement of critical objectives (Gibson et al., 2004, p.2).

"A tool that can be employed to provide greater confidence that the outputs of processes and services can be delivered in the face of risks. It is concerned with identifying and managing the risks which threaten to disrupt essential processes and associated services, mitigating the effects of these risks, and ensuring that recovery of a process or service is achieved without significant disruption to the enterprise" (Gibb & Buchanan, 2006, p. 129).

- "The ongoing management of the business continuity plan to ensure the it is always current and available and
- The ongoing management of operational resilience and process availability within an organisation, with the aim of ensuring that the organisation experiences the minimum possible day-to-day disruption" (Continuity Central, 2008)

Finally, the definition used by Verdonck, Klooster & Associates is: 'Business Continuity Management encompasses the management process that aims to prevent severe disruptions in the business and to protect critical processes against the consequences of disruptions or disasters' (Scheffel, 2004).



Although there is no commonly accepted definition for BCM, we can identify some characteristics of BCM that can be encountered in all the definitions and/or the accompanying explanations.

These characteristics are as follows:

- The aim of any BCM is to ensure the continuity of the business at a certain minimum level;
- BCM initiatives should be directed towards the critical business processes;
- BCM encompasses both the prevention of disasters or disruptions and limiting the damage to business in case of a disaster or disruption, so it's has preventive, corrective and repressive characteristics;
- BCM is a continuous management process, not a single project.

## **2.4 HIGH LEVEL PRINCIPLES OF BUSINESS CONTINUITY**

In the summer of 2004, the Financial Stability Forum and the Bank of England co-hosted a symposium on business continuity issues. Based on the findings of the symposium, the Financial Stability Forum asked the sectoral standard setting bodies (the Basel Committee on Banking Supervision (BCBS), the International Organisation of Securities Commissions (IOSCO) and the International Association of Insurance Supervisors (IAIS)) or the Joint Forum to review approaches to business continuity across countries and financial sectors and consider whether it might be appropriate to develop high-level principles that could apply across the financial system globally (Bank for International Settlements, 2005).

The Joint Forum's parent organisations (BCBS, IOSCO and IAIS) confirmed in November 2004 that the Joint Forum should undertake such a review. Following an initial scoping exercise, the Joint Forum concluded in February 2005 that high-level principles on business continuity would contribute beneficially to the resilience of the global financial system.

The high-level principles that follow are applicable to both financial industry participants and financial authorities except for Principle 7, which is relevant only for financial authorities. Because of the different perspectives, roles and responsibilities of these two groups of organisations in the event of a major operational disruption, however, the way in which a particular principle applies may be different. The key differences in application are highlighted in the discussion that follows each principle.

- Principle 1 emphasises that the requirement for sound business continuity management applies to all financial authorities and financial industry participants and that the ultimate responsibility for business continuity management – not unlike the management of other risks – rests with an organisation's board of directors and senior management.<sup>1,2</sup>
- Principle 2 advises organisations that they should explicitly consider and plan for major operational disruptions. While this concept may be new for many

---

<sup>1</sup> This paper refers to a management structure comprising a board of directors and senior management. It is recognised, however, that there are significant differences in legislative and regulatory frameworks across countries as regards the functions of the board of directors and senior management. In some countries, the board has the main, if not exclusive, function of supervising the executive body (senior management, general management) so as to ensure that the latter fulfils its tasks. For this reason, in some cases, it is known as a supervisory board. This means that the board has no executive functions. In other countries, the board has a broader competence in that it lays down the general framework for the management of the bank. Owing to these differences, the terms "board of directors" and "senior management" are used in this paper not to identify legal constructs but rather to label two decision-making functions within an organisation.

<sup>2</sup> Not all *financial authorities* have boards, in which case references to the board or the board and senior management should be read to mean senior management.

organisations, it is considered important in light of the increasing frequency of such events.

- Principle 3 states that financial industry participants should develop recovery objectives that reflect the risk they represent to the operation of the financial system.

Financial industry participants that provide critical services to, or otherwise present significant risk to the operation of, the financial system should target higher standards in their business continuity management than other participants. This concept may be new for some financial industry participants. Because the steps necessary to improve the resilience of the financial system may be more costly than the steps such participants would choose to undertake on their own, financial authorities are encouraged to participate, as appropriate, in identifying recovery objectives that are proportionate to the risk posed by a given participant in order to achieve a reasonably consistent level of resilience.

- Principle 4 stresses the critical importance of business continuity plans addressing the full range of internal and external communication issues an organisation may encounter in the event of a major operational disruption. The principle specifically recognises that clear, regular communication during a major operational disruption is necessary to manage a crisis and maintain public confidence.
- Principle 5 highlights the special case of cross-border communications during a major operational disruption. Given the deepening interdependencies of financial systems across national boundaries, this principle advises financial industry participants and financial authorities to adopt communication

protocols that address situations where cross border communication may be necessary.

- Principle 6 emphasises the need to ensure that business continuity plans are effective and to identify necessary modifications through periodic testing.
- Finally, to ensure that financial industry participants are in fact implementing appropriate approaches to business continuity management that reflect the recovery objectives adopted in accordance with Principles 1 and 3, Principle 7 calls upon financial authorities to incorporate business continuity management reviews into their frameworks for assessing financial industry participants (Bank for International Settlements, 2005).

#### **2.4.1 Principle 1: Board and senior management responsibility**

Financial industry participants and financial authorities should have effective and comprehensive approaches to business continuity management. An organisation's board of directors and senior management are collectively responsible for the organisation's business continuity.

Business continuity management should be an integral part of the overall risk management programme of financial industry participants and financial authorities. Business continuity management policies, standards and processes should be implemented on an enterprise-wide basis or, at a minimum, embedded in an organisation's critical operations.

Comprehensive business continuity management addresses not only technical considerations but also the human dimension, recognising that employees and possibly their families will be affected by the same event that gives rise to business continuity concerns.

The personal safety of staff should be the paramount consideration of an organisation's business continuity plan.

An organisation's board and senior management are responsible for managing its business continuity effectively and for developing and endorsing appropriate policies to promote resilience to, and continuity in the event of, operational disruptions. They should recognise that outsourcing a business operation does not transfer the associated business continuity management responsibilities to the service provider. The board and senior management should create and promote an organisational culture that places a high priority on business continuity. This message should be reinforced by providing sufficient financial and human resources to implement and support the organisation's approach to business continuity management.

A framework should be implemented for reporting to the board and senior management on matters related to business continuity, including implementation status, incident reports, testing results and related action plans for strengthening an organisation's resilience or ability to recover specific operations. An organisation's business continuity management should be subject to review by an independent party, such as internal or external audit, and significant findings should be brought to the attention of the board and senior management on a timely basis.

Confusion can be a major obstacle to an effective response to an operational disruption (Bank for International Settlements, 2005). Accordingly, roles, responsibilities and authority to act, as well as succession plans, should be clearly articulated in an organisation's business continuity management policies. Senior



management should recognise that they may need to re-align priorities and resources during a disruption in order to expedite recovery and respond decisively. It is important that a locus of responsibility for managing business continuity during a disruption is established, such as a crisis management team with appropriate senior management membership. In addition, senior management should be involved in communicating the organisation's response, commensurate with the severity of the disruption.

In the case of financial authorities, the board and senior management should be confident in the authority's ability to fulfil its mandate during an operational disruption that affects its own operations or those of the financial system. Accordingly, they should be satisfied that the authority's powers provide for sufficient flexibility to respond appropriately and expeditiously to the wide range of issues that might arise under such circumstances.

Given the interdependencies within financial systems, it would be useful for financial authorities that share oversight responsibilities for a given financial system to agree on a framework for coordinating the response to major operational disruptions affecting that system.

#### **2.4.2 Principle 2: Major operational disruptions**

Financial industry participants and financial authorities should incorporate the risk of a major operational disruption into their approaches to business continuity management. Financial authorities' business continuity management also should address how they will respond to a major operational disruption that affects the

operation of the financial industry participants or financial system for which they are responsible.

Major operational disruptions pose a substantial risk to the continued operation of financial industry participants and financial authorities, as well as to the operation of the financial system. Accordingly, all financial industry participants and financial authorities should incorporate the risk of a major operational disruption in their business continuity plans. The extent to which a financial industry participant prepares to recover from a major operational disruption should be based on its unique characteristics and risk profile. Because access to the resources needed for the full recovery of its operations may be limited during a major operational disruption, a financial industry participant should identify through a business impact analysis those business functions and operations that are to be recovered on a priority basis and establish appropriate recovery objectives for those operations.

During a major operational disruption, the operation of the financial system will be of keen importance nationally and, possibly, globally. A financial authority will be expected to play a major role in monitoring the status of the financial markets and financial industry participants for which it is responsible. Depending on its mandate, a financial authority might also be expected to coordinate efforts to recover critical services to the financial system.

Major operational disruptions vary in intensity and scope. In many cases, organisations may be able to remain at their primary business locations if they have sufficient backup for power and other essential services. Recent experience, however, has demonstrated that some major operational disruptions constitute



extreme events whose impact can be very broad. In evaluating whether their own business continuity management is sufficient to accommodate such major operational disruptions, financial industry participants and financial authorities should review the adequacy of their recovery arrangements in three important areas. First, an organisation should take care that its alternate site is sufficiently remote from, and does not depend on the same physical infrastructure components as, its primary business location. This minimises the risk that both could be affected by the same event. For example, the alternate site should be on a different power grid and central telecommunication circuit from the primary business location. Second, an organisation should consider whether the alternate site would have sufficient current data and the necessary equipment and systems to recover and maintain critical operations and services for a sufficient period of time in the event that its primary offices are severely damaged or access to the affected area is restricted. Third, given that staff at the primary business location are likely to be unavailable, the business continuity plan should address how the organisation will provide sufficient staff – in terms of number and expertise – to recover critical operations and services consistent with its recovery objectives. Some approaches to ensuring that sufficient staff are available at alternate sites include: locating staff at alternate sites on a permanent basis (eg in the case of load-sharing), cross-training employees at alternate sites or from other locations, ensuring that a percentage of employees deemed essential to meeting recovery objectives are located away from the primary business location at any given time, and hiring employees who live at the outer edges of typical commuting ranges from the primary business location.

### **2.4.3 Principle 3: Recovery objectives**

Financial industry participants should develop recovery objectives that reflect the risk they represent to the operation of the financial system. As appropriate, such recovery objectives may be established in consultation with, or by, the relevant financial authorities.

A financial industry participant that experiences a major operational disruption might affect the ability of other financial industry participants – and possibly the financial system – to continue normal business operations. Accordingly, financial industry participants should consider the extent to which they pose such a risk and augment their business continuity management where they determine that a disruption of their operations would affect the operation of the broader financial system. Relevant financial authorities are encouraged to provide guidance that would assist financial industry participants in making this assessment. Examples include a payment and settlement system operator on which financial industry participants depend to process and complete transactions – particularly where there are no others capable of substituting for that operator – or financial industry participants that play a significant role in providing financial services within a particular region.

Financial industry participants should establish recovery objectives that are proportionate to the risk they pose to the operation of the financial system. The responsibility for setting recovery objectives rests with the organisation's board and senior management. Financial authorities are encouraged to participate in the

identification of recovery objectives where such a role is consistent with an authority's mandate. The highest recovery objectives typically should be reserved for those financial industry participants that are most likely to disrupt the financial system in the event of a major operational disruption because of the critical services they provide or their significance to the financial system in which they operate. For example, critical market participants might reasonably be held to a within-the day-of-disruption recovery time objective, and expected not only to recover critical operations and services but also to resume new business within the same timeframe. It may be acceptable for other participants to target a less stringent recovery time depending on the impact a disruption of their operations would have on the financial system or on the expectations of other financial industry participants. In assessing the reasonableness of an organisation's recovery objectives, financial authorities are strongly encouraged to consider the increased risk of failed transactions, liquidity dislocations, solvency problems, and loss of confidence that accompany prolonged disruptions in the financial system.

Recovery objectives should identify expected recovery levels and recovery times for specific activities. Although they may not be achievable in every circumstance, recovery objectives provide financial industry participants with benchmarks for testing the effectiveness of their business continuity management. They also provide some assurance that financial industry participants representing similar external risks will attain a consistent level of resilience. When identifying recovery objectives, it would also be appropriate to identify appropriate timeframes for implementing those objectives.

#### **2.4.4 Principle 4: Communications**

Financial industry participants and financial authorities should include in their business continuity plans procedures for communicating within their organisations and with relevant external parties in the event of a major operational disruption.

The ability to communicate effectively with relevant internal and external parties in the event of a major operational disruption is essential for financial industry participants and financial authorities alike. Particularly in the early stages of a disruption, effective communication is necessary to gauge the impact of the disruption – on an organisation’s staff and operations, and on the broader financial system – and make appropriate decisions about whether to invoke a business continuity plan. As time progresses, the ability to communicate the best available information to the appropriate parties in a timely fashion is critical to the recovery of an organisation’s operations and to the return of the broader financial system to normal operation. Maintaining public confidence, whether in an individual financial industry participant or in the financial system as a whole, requires clear, regular communication throughout the duration of a major operational disruption.

Accordingly, and also because of the added pressure that is often associated with decision-making during a major operational disruption, the business continuity plans of financial industry participants and financial authorities should incorporate comprehensive emergency communication protocols and procedures. For example, a financial industry participant would need to consider how best to communicate within its organisation as well as with relevant financial authorities, other financial

industry participants, the public and other stakeholders. It may also be necessary for a participant to obtain information from financial authorities and other financial industry participants regarding the status of the financial system. A financial authority will need to consider similar issues, but its emergency communication procedures should also reflect its broader responsibilities. For example, a financial authority may want to consider issuing public statements during a crisis to assure the markets and the public that appropriate measures are being taken and inform them of those measures.

The communication procedures of financial industry participants and financial authorities generally should:

- Identify those responsible for communicating with staff and various external stakeholders. This group might include senior management, public affairs staff, legal and compliance advisors, and staff responsible for the organisation's business continuity procedures. This group should be able to communicate with personnel located at isolated sites, dispersed across multiple locations, or otherwise away from the primary business location;
- Build on any communication protocols that already exist within the financial system and include contact information for relevant domestic financial authorities and financial industry participants to facilitate an assessment of the condition of the financial system and coordinate recovery efforts. Examples of existing communication protocols might include conference call schedules developed by financial sector trade associations or financial authority working groups and bilateral communication procedures between major international exchanges. In addition, consideration should be given to including contact



information for officials with local emergency response organisations where critical facilities are located;

- Address related issues that can arise during a major operational disruption, such as how to respond to failures in primary communication systems. This could include, for example, developing systems and contact information for key personnel that would facilitate multiple methods of communicating (e.g. digital and analogue land line phones, mobile phones, satellite phones, text messaging, websites, hand-held wireless devices, etc);
- In the case of financial authorities, include, as appropriate, contact information for national or regional protection and intelligence agencies. These arrangements may require the use of secure communications using specialised “secure” telephones, faxes, and emails; and,
- Provide for the regular updating of calling trees and other contact information and the periodic testing of calling trees.

#### **2.4.5 Principle 5: Cross-border communications**

Financial industry participants’ and financial authorities’ communication procedures should address communications with financial authorities in other jurisdictions in the event of major operational disruptions with cross-border implications.

Because of the deepening interdependencies among financial industry participants across jurisdictions, it is increasingly likely that the impact of a major operational disruption will extend across national borders. Addressing disruptions that cross national borders introduces additional complexity. Although domestic communication procedures may be reasonably well-defined in the business



continuity plans of many financial industry participants and financial authorities, special attention is warranted in preparing for disruptions with international scope.

Financial industry participants should consider the possibility that a disruption of their business operations in one jurisdiction would affect significant subsidiary or branch operations or otherwise affect the financial system in other jurisdictions. Where this outcome is possible, a financial industry participant's communication protocols should address the circumstances under which it would contact the relevant non-domestic financial authorities.

Financial authorities should incorporate communication protocols in their business continuity plans for communicating with financial authorities in other jurisdictions in the event of a major operational disruption that affects (or could affect) the continued operation of the international financial system. Although it was developed to address financial crises and not business continuity events, per se, the Memorandum of Understanding on co-operation between the Banking Supervisors, Central Banks and Finance Ministries of the European Union in Financial Crisis situations (2005) provides a useful example of what such communication protocols might entail. It comprises a set of principles and procedures for sharing information, views and assessments among the authorities potentially involved in a crisis situation, as well as arrangements for the development of contingency plans for the management of crisis situations as well as stress testing and simulation exercises.

These communication protocols should build on existing cross-border relationships and multi-jurisdictional protocols by identifying the types of officials at financial authorities who might need to be involved in responding to such disruptions and

including the relevant contact information. Examples of existing contact lists include the Crisis Management Contact List maintained by the Financial Stability Forum covering central banks, supervisory agencies, finance and treasury departments, and key international financial institutions in some 30 countries and the Bank Supervisors' Contact List maintained by the BCBS listing supervisory contacts around the world. It is likely that communication with financial authorities in other jurisdictions would take place at several levels simultaneously, with senior decision-makers and more technical or specialised staff members in one organisation holding discussions with their respective counterparts at the other.

Financial authorities, in particular, are encouraged to hold periodic discussions with relevant financial authorities in other jurisdictions to develop a shared understanding of the events that could have significant cross-border effects on the financial system and agree on procedures for communicating with one another under such circumstances and the issues that should be addressed. The issues that might be covered in the event of cross-border disruptions would include, for example, the impacts of the disruption in their respective markets and its contagion effects, if any; issues involving emergency closures or suspensions of major markets; changes in trading hours or clearing and settlement periods; and, the details of any regulatory forbearance that may have been extended.

#### **2.4.6 Principle 6: Testing**

Financial industry participants and financial authorities should test their business continuity plans, evaluate their effectiveness, and update their business continuity management, as appropriate.

Testing of the ability to recover critical operations as intended is an essential component of effective business continuity management. Such testing should be conducted periodically, with the scope and frequency determined by the criticality of the applications and business functions, the organisation's role in broader market operations, and material changes in the organisation's business or external environment. In addition, such testing should identify the need to modify the business continuity plan and other aspects of an organisation's business continuity management in response to changes in its business, responsibilities, systems, software, hardware, personnel, or facilities or the external environment. An independent party, such as internal or external audit, should assess the effectiveness of the organisation's testing programme, review test results and report their findings to senior management and the board.

Financial authorities should strongly encourage financial industry participants that present risk to the financial system to conduct tests from their alternate sites with relevant critical market participants and payment and settlement system operators. Financial authorities and key financial industry participants are also encouraged to participate in market- or industry-wide tests to assess the level of resilience across markets and the compatibility of the recovery strategies of individual participants. In

light of the substantial costs involved, the decision to undertake a market- or industry-wide test should be based on a thorough cost-benefit analysis.

In addition to ensuring that business continuity plans are constantly evaluated and updated, testing is also essential for promoting awareness, familiarity and understanding among key personnel of their roles and responsibilities in the event of a major operational disruption. It is important, therefore, that testing programmes should involve all personnel who are likely to be involved in responding to major operational disruptions.

#### **2.4.7 Principle 7: Business continuity management reviews by financial authorities**

Financial authorities should incorporate business continuity management reviews into their frameworks for the ongoing assessment of the financial industry participants for which they are responsible.

Financial authorities should expect financial industry participants to develop and implement effective business continuity management that is updated on an ongoing basis. Financial authorities should incorporate business continuity management reviews into their frameworks for the assessment of financial industry participants.

The scope and frequency of the reviews will be determined by the requirements of their regulatory or supervisory frameworks. Assessments should give due consideration to whether a participant's business continuity management, including its recovery objectives, is appropriate for the size and scope of its business and the risk the participant presents to the continued operation of the financial system.

Financial authorities should also assess whether participants are taking appropriate steps to augment their business continuity management, where necessary. Where financial authorities share responsibility for the same financial industry participant, it would be useful for those authorities to agree on a framework for coordinating those reviews.

In the course of reviewing a participant's business continuity management, a financial authority should assess whether the testing programme provides adequate assurance that business processes can be recovered as intended.

## **2.5 NEED FOR BCM**

A description of the need for BCM is already enclosed in the term itself. Organizations occupy themselves with BCM to assure the continuity of their business. Although the need for continuity of business exists for just as long as business itself, BCM is a relatively new concept compared to most other business disciplines. BCM has been developed out of its predecessors disaster recovery, which was born in the 1960's paired with the rising computerization and later contingency planning.

Interest in BCM came up in the 1990's, but actually has only gained real momentum over the last several years. The reason for this is twofold: on one side, an increasing pressure is exerted on organizations to provide assurance for the continuity of their business processes. This is principally caused by two changes in the business environment, namely rising competition and higher demands of customers and increasing regulatory requirements.

At the same time, the assurance of the continuity becomes more and more complex for organizations. Three changes that have caused this can be identified, namely increasing threats, increasing supply and demand chain integration and increasing dependency of business processes on complex information systems (Noakes-Fry & Diamond, 2001; Leegwater & Reiniers, 2005; Leegwater & Ploeg, 2005).

Besides the five changes mentioned above, there is one other change that has influenced the advent of BCM. Although the advent of process-based approaches (Leegwater & Ploeg, 2005) did not directly cause the advent of BCM, it did cause a shift in management thinking which enabled the process focus of BCM.

### **2.5.1 Rising competition and higher demands of customers**

Rising competition and higher demands of customers, such as the expectation of 24/7 availability of (digitalized) services makes it necessary for organizations to pay extra attention to their continuity assurance. A disruption of business can have severe consequences such as financial loss and loss of credibility or goodwill for the organization concerned. Customers can also explicitly demand certain assurance with regard to the continuity of their suppliers and do so to an increasing extent.

### **2.5.2 Increasing threats**

The threats that endanger the continuity of a business are increasing. Incidences of terrorism, disasters, fraud and commercial espionage have increased in recent years. (CCTA, 1995-1) Besides an increase of the threats themselves, we can also observe an increase in the visibility of the threats and their consequences. This is largely



caused by the extensive media attention. This extra visibility reinforces the effect that the increasing threats have on the awareness within organizations.

### **2.5.3 Increasing supply and demand chain integration**

Organizations choose to focus more and more on their core activities and outsource non-core activities. This is due to the rising competition, which leads to a need for cost efficiency. This extension of the supply and demand chains accompanied by the high demands regarding delivery time, quality and price obliges chain partners to cooperate more intensively. As chain partners increasingly integrate their processes with each other, the consequences of discontinuity also get extended. The effect of discontinuity is not limited to one party but can also have consequences for the entire chain. This has to be taken into account when planning for continuity.

### **2.5.4 Increasing dependency on complex information systems**

Organizations depend more and more on their information systems and underlying infrastructures, including (data) communication facilities. This rising dependency on IT and other technologies makes organizations more vulnerable to disruptions in these technologies. An obvious example of this dependency can be seen in the Y2K threat that caused great commotion within many organizations and was followed by a substantial rise in BCM activities.

### **2.5.5 Advent of process based approaches**

The need for more continuity played a major role in the development of BCM. Besides that, an important change in organizational thinking also has to be mentioned. As opposed to concepts like disaster recovery and information security,

BCM focuses on (critical) processes instead of business functions. This process focus has been enabled by the advent of the process-based approaches, like Business Process Reengineering/Redesign (BPR), Business Process Improvement (BPI) or Total Quality Management (TQM) and led to an important shift in organizational thinking. Organizations started to realize they should focus not only on business functions but also, and may be even mainly, on business processes, since processes create the value organizations aim for.

In summary, we can state that changes that result in increasing pressures to provide continuity assurance, together with changes that make it more difficult to assure this desired continuity, form an impulse that resulted in the advent of BCP. The change in management thinking that led to process based approaches also was an important enabler for the advent of BCP.

## **2.6 EFFECTIVE BUSINESS CONTINUITY MANAGEMENT**

Business continuity management is a whole-of-business approach that includes policies, standards, and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption (Bank for International Settlements, 2005). Its purpose is to minimise the operational, financial, legal, reputational and other material consequences arising from a disruption. Effective business continuity management concentrates on the impact, as opposed to the source, of the disruption, which affords financial industry participants and financial authorities greater flexibility to address a broad range of disruptions. At the same time, however, organisations cannot ignore the nature of the risks to which they are exposed.

For example, organisations located in earthquake-prone regions commonly plan for the impact of earthquake-related major operational disruptions.

Effective business continuity management typically incorporates business impact analyses, recovery strategies and business continuity plans as well as testing programmes, training and awareness programmes, and communication and crisis management programmes (Bank for International Settlements, 2005).

- A business impact analysis is the starting point – it is a dynamic process for identifying critical operations and services, key internal and external dependencies and appropriate resilience levels. It assesses the risks and potential impact of various disruption scenarios on an organisation's operations and reputation.
- A recovery strategy sets out recovery objectives and priorities that are based on the business impact analysis. Among other things, it establishes targets for the level of service the organisation would seek to deliver in the event of a disruption and the framework for ultimately resuming business operations.
- Business continuity plans provide detailed guidance for implementing the recovery strategy. They establish the roles and allocate responsibilities for managing operational disruptions and provide clear guidance regarding the succession of authority in the event of a disruption that disables key personnel. They also clearly set out the decision-making authority and define the triggers for invoking the organisation's business continuity plan.

## **CHAPTER THREE**

### **METHODOLOGY**

#### **3.1 INTRODUCTION**

This chapter is organized into two parts. The first part considers the profile of SG-SSB which served as the case study institution. It basically looks at its history and corporate mission as well as its Business Continuity Plan manual. The second part looks at the actual methodology. It looks at the sources of data, data analysis and presentation, sampling design and technique.

#### **3.2 SG-SSB LIMITED AS THE CASE STUDY**

##### **3.2.1 Brief History of SG-SSB Limited**

SG-SSB Ltd was formed through the acquisition of SSB Bank by Société Générale. The integration of SSB Bank within Société Générale's international network enabled SSB Bank to strengthen its position in the Ghanaian financial industry.

The Bank is represented in every region in Ghana with 38 fully-networked branches. The Bank has a very strong representation in the Western Region with eleven branches to provide financial support to the cocoa growing areas.

The competitive advantage of the bank is manifested through its values of Professionalism, Team Spirit and Innovation. It also pursues a balanced growth strategy for its deposits, credits, retail and corporate services based on a strong network of its branches.

### **3.2.2 Corporate Mission of the Bank**

The mission of SG-SSB is to create the preferred banking institution, which employs professionalism, teamwork and innovation to provide quality products and services that best satisfy the needs of its customers. To achieve this, values that relate to the mission have been made clear. These are:

- Aiming for enhanced shareholder value
- Focusing on quality
- Rewarding success
- Identifying with the group network
- Commitment to local communities and
- Achieving excellence

### **3.2.3 Operational Risk and Permanent Control Department**

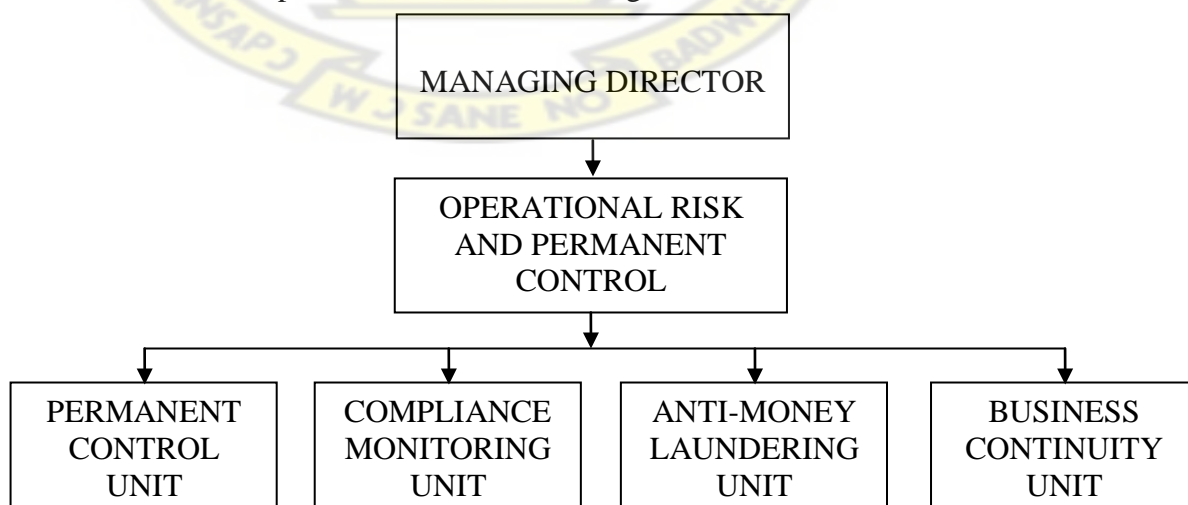
The Business Continuity Unit of SG-SSB Limited is under the direct supervision of the Operational Risk and Permanent Control Department. The primary function of the Operational Risk and Permanent Control Department is to manage the Bank's all risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events, including events of low probability of occurrence, but with a risk of high loss as defined by the Basel II Accord (the second of the Basel Accords which are recommendations on banking laws and regulations issued by the Basel Committee on Bank Supervision)

The Operational Risk and Permanent Control Department consists of Permanent Supervision Unit; Compliance Monitoring Unit, Anti-Money Laundering Unit; and Business Continuity Unit.

The Business Continuity Unit through the BCP Manager plays the following roles;

- Organise and supervise the planning processes, the creation of the BCP and its testing, training and ongoing maintenance: and
- Coordinate the IT BCP in order to adapt properly the capacity of the IT backup relative to the banking needs. Must act in the choice of the IT backup site and in the analysis of “disaster risks” of this site compared to the risks identified on the IT production site.
- Act as the Alert Correspondent, the point of contact for any alert concerning the bank and shall:
  - Receive alerts and perform an initial qualification
  - Transmit the alert to the Crisis Director, if necessary
  - Propose the configuration of the mechanism to be deployed
  - Deploy the crisis mechanism, following the Crisis Director’s decision
  - Inform the parent company (SG) should the subsidiary’s Crisis Management Team be activated.

The structure of the department is shown in the Figure 3.1 below;



**Figure 3.1 The Structure of the Operational Risk and Permanent Control Department**



### **3.2.4 Business Continuity Plan Manual for SG-SSB Limited**

#### **3.2.4.1 Policy**

The policy of SG-SSB is to maintain a Business Continuity Plan that will ensure prompt and efficient recovery of its essential business operations from any disaster occurring at its premises which results in:

- Non-access to premises
- Unavailability of IT systems
- Staff unavailability

#### **3.2.4.2 Recovery Overview**

To meet predefined crisis scenarios, the SG-SSB BCP addresses two issues,

- The continuity of banking activities (called “BCP-Banking”);
- IT backup (called: “BCP-IT”)

The banking BCP is to enable the bank continue its activities safely on the usual work place or in another place (depending on the crisis) called recovery site. The banking BCP address the following:

- Activities of the Head Office
- Activities of the Branches

The IT BCP is to enable the bank IT applications to continue functioning in a crisis situation.

#### 3.2.4.2.1 *Recovery Objectives and Plan Scope*

The Bank Business Continuity Planning that is, planning for recovery from a disaster aims at:

- Managing the risks which could result in disastrous events and thus minimise the likelihood of a disaster occurring;
- Reducing the time taken to recover when an incident occurs; and
- Minimise the risks involved in the recovery process by making the critical decisions in advance in stress-free conditions.

##### 3.2.4.2.1.1 Objectives

The objectives of the plan are to:

- Provide for the safety and wellbeing of people in the branch and department at the time of a disaster.
- Establish management succession and emergency powers.
- Identify critical businesses and supporting functions;
- Facilitate the successful recovery of each essential business operations normally carried out at the Bank.
- Keep all staff in the business areas informed of what to do in the event of a disaster.

##### 3.2.4.2.1.2 Scope

This plan covers situations where individual business locations are impacted by an incident. It does not cover Large-scale crisis where, a whole city, region or country is

impacted by a major crisis. It is anticipated to develop later a “resilience” strategy to handle such scenarios.

#### *3.2.4.2.2 Recovery Strategies*

The main contingencies the strategy will cover are:

- Non-access to premises-It is the non-access to a floor or the building of the work place of the bank staff
- Unavailability of IT systems-An IT failure (software/equipment) with IT servers, a computer virus (in some circumstances), a power cut or a telecom failure.
- Staff unavailability-In case of an epidemic or a pandemic, the bank remains very sensitive to the absence of its staff.

##### *3.2.4.2.2.1 Banking BCP Strategy-Head Office*

Essential operations will be recovered within 24hours of declaring a disaster by relocating staff and necessary resources to designated Recovery Centers, where fully equipped office accommodation including PCs and terminals with on line connection to the Bank’s systems will be available.

##### *3.2.4.2.2.2 Banking BCP Strategy-Branch*

In the case of Branches, the essential activities of the Incident branch would be merged with that of a designated recovery branch within 15km radius of the incident branch. Where there are no designated recovery branches within 15km radius a temporary location needs to be identified and setup within 5days.

#### 3.2.4.2.2.3 IT BCP Strategy

IT systems may need to be recovered or restored in the event of an IT related incident.

These incidents may be grouped as;

- Data center Incident,
- Wide Area Network Failure and
- IT failure at Branch or Department.

In the event of an IT Failure at Branch or Department, the Banking BCP strategy above would be activated if the incident is not resolved within 24 hours. A fully mirrored duplicate site would also have an alternative network.

#### 3.2.4.2.3 Recovery Teams and Roles

During the Recovery Phase, the normal organisational structure will be suspended and replaced by the Crisis Organisation which will concentrate on maintaining vital business operations. This organisation would consist of the following:

- Crisis Management Team
- Incident Control Group
- Business Unit's Recovery Team

##### 3.2.4.2.3.1 Crisis Management Team

The Crisis Management Team activates a “backup and recovery” suited to the crisis situation. The Crisis Management Team is the sole entity for deciding whether to activate a BCP mechanism. The Crisis Management Team may meet in order to manage a crisis, without necessarily activating a BCP mechanism.

#### 3.2.4.2.3.2 Incident Control Group

Incident Control Group (ICG) at the branch and departments is responsible for dealing with the immediate physical effects of an actual or threatened disaster, for example fire or flood or IT system failure. The ICG would have authority to:

- Order people to leave the premises;
- Request them to assist the ICG or with other emergency procedures following evacuation, provided it is safe and reasonable to do so.

The main responsibilities of the ICG are to:

- Prevent the incident from escalating into a disastrous event if it is little more than a threat; or
- Control the extent of potential damage if the escalation cannot be prevented and
- Inform the Crisis Management Correspondent or Deputy if any incident
- Ensure safety and welfare of Branch staff during and its aftermath.

#### 3.2.4.2.3.2 Business Unit Recovery Team

The Business Unit's Recovery Team (BURT) are the nominated members of their business unit's who are to organise and manage the recovery of the business unit's operations following a disaster at a recovery location.

#### 3.2.4.2.4 *Recovery Procedures*

In case of an important alert, The ICG will contact the Crisis Management Correspondent or the Deputy, who will immediately inform the Crisis Director, who determines the appropriate actions to be taken. If the Crisis Management Team is activated, the Crisis Management Correspondent or the Deputy shall inform the BHFM<sup>3</sup>/Paris alert Correspondent.

At appropriate points the ICG should also ensure the necessary emergency procedure actions have been carried out, for example:

- Fire/emergency evacuation procedures;
- Calling the Emergency Services; and
- Removal of valuable objects;

The ICG, using the cascade staff callout system, will contact the BURT who will take part in the business recovery. If necessary, arrangements should be made to transport staff to the Recovery Center. On arrival each Recovery Team will start its own recovery procedures.

Each business unit would have to develop procedures to cover:

- Alert Management
- Evacuation
- Recovery process for critical activities.

---

<sup>3</sup> BHFM – Banque hors de France Métropolitain (the International Retail Banking Division)



#### **3.2.4.3 Communication Procedures**

Communicating with external contacts (excluding emergency services) regarding the incident and its effects on the bank's business will be dealt with by the External Communication Department in conjunction with senior management.

However, where appropriate, it may be necessary to communicate with clients, regulators or other outside organisations directly, in order to update them of the situation. Staff are to check with External Communication Department before giving out any information about the incident or its effects on SG-SSB.

If the press arrive during an incident they should be referred to the External Communication Department. All business units are to instruct their staff to refer all media approaches to their managers. If approached by the media, staff should not:

- make statements without approval;
- divulge any information other than simple confirmation of the incident which has occurred.
- speculate;
- give out casualty members or names

#### **3.2.4.4 Return to Normal Operations**

When it is advised that the premises are ready for reoccupation, arrangements for the return need to be planned.

Staff need to be instructed to:

- save all data for transfer to original premises;
- delete Department data from the Recovery Center's PCs; and
- remove Departmental and personal property from the Recovery Center.

#### *3.2.4.4.1 Review of Events*

After the end crisis situation a review with the Team Leaders and Management must be held on, the disaster, the recovery and the performance of the BCP to identify any measures for prevention of future occurrences and improvements to the BCP.

#### *3.2.4.5 BCP Testing and Review*

The ability of the BCP to be effective in business interruptions situations can only be assessed if testing is carried out. The purpose of a BCP test is to demonstrate the overall recovery ability of an area during a simulated major interruption of service (s) and to verify that the information in the BCP procedures is correct.

The BCP procedure should be reviewed with each business unit's manager to identify changes and check that the business unit's recovery requirements are still valid.

##### *3.2.4.5.1 Objective of Test*

1. Determine the feasibility and compatibility of recovery facilities, BCP procedures and supporting manual workarounds;
2. Identify areas in the BCP procedures that need to be modified;
3. Provide training to the Recovery teams thus ensuring that all the key players receive practical experience

4. Demonstrate the ability of the business unit/department (s) to recover;
5. Demonstrate the ability of IT service providers to meet business expectations.

#### 3.2.4.5.2 *Test Strategy*

In general tests would start small and progress to full tests. The following methods would be used:

- Walkthrough - The participants sit round a table, each with a copy of the BCP (or appropriate part of the BCP), and ‘walk’ through it by reading and discussing which part in sequence. The objective is to identify any weaknesses, errors and omissions in the procedures. This needs to be done by each business unit at least three times a year. Participants should be
  - the key staff in the operation concerned and its Recovery Team;
  - other staff who are knowledgeable about the operation and the way it fits into the organisation.
- Scenario Workshop - The test participants are gathered around a conference table and told that a specific business interruption has occurred/ while seated at the table, they “walk through” the interruption to verify that the BCP contains the materials necessary to continue the delivery of mission critical services.

This test would be done at least two times in a year. The Scenarios should be designed around the actual conditions of the business and its operations and to introduce any possible disaster in realistic way. Participants of the test would involve:

- Crisis Committee
  - The Incident Control Group
  - Business Unit Recovery Team
- Simulation of a Live Test - This involves creating a simulated business interruption event. During this simulation, those involved in the test will act as if the simulated event has occurred and will operate under the BCP. These tests would be done at least once in a year and would be help outside normal working hours so that resources can be used without affecting normal operations. It must be as near to real life as possible so that all aspects of the BCP are tested.

#### **3.2.4.6 Limitations**

This manual only provides the framework to guide the banks Departments in drafting their BCP actions. It does not provide step by step actions to be done by the business units. Each business unit would be responsible for drafting detailed procedures addressing actions to be carried out in the event of a disaster.

### **3.3 METHODOLOGY**

This section details the approach adopted to obtain data to answer the research questions raised in chapter one, and to achieve the objectives of the research.

#### **3.3.1 Research Setting**

The research was conducted within the Operational and Permanent Control Department as well as the entire branches and departments of the bank. The primary

focus was on SG-SSB Limited and the case study approach was used in the study which enabled an appreciable level of investigation within the limited time.

### **3.3.2 Sources of Data**

This study uses both primary and secondary data. The primary data was obtained from fieldwork. Questionnaires were administered to some staff of SG-SSB; BCP representatives of the various branches and departments and a random sample of staff who are non-BCP representatives. A questionnaire was also administered to the BCP manager of the bank and oral interview was held with the manager as well. These constituted vital sources of primary data for the study.

Secondary data was obtained from journals, textbooks, annual reports, and relevant websites on Business Continuity Planning for Financial Institutions.

### **3.3.3 Study Population**

The study population was made up of management and entire employees of the Bank at the various branches and Head Office Departments. The population size was seven hundred and forty (740).

### **3.3.4 Sample Size**

Economically, it is not feasible to seek the views of every member of this population. To follow the practices of research, a sample was taken from the population. Adopting a convenient purposive sampling approach, a sample size of 100 was targeted and this was proportioned among BCP Manager (1), BCP Representatives at the 45 Branches and Agencies of the Bank (45), and a random sample of staff who are non-BCP representatives from various Departments of the Bank (54). The sample constituted about 13.5% of the population. This sample size was chosen because of the busy nature of staff and the limited time frame for the study.

### **3.3.5 Sampling Design and Technique**

Principally, the simple, purposive and stratified random sampling approaches were used.

The simple random sampling technique postulates that each element or member of the population has an equal and the same chance of being selected in the sample. With this sampling method all the elements or members in the population are assumed to have the same characteristics. Non-BCP representatives were randomly selected from various departments of the bank

With stratified random sampling technique, the BCP representative of each stratum, branch in this case was included in the sample. This ensured a fair representation of all branches in the sampling. The BCP representatives were targeted purposively because the project falls directly under their remit.

In the light of this, the required samples were picked from the list of employees in the branches and departments and heads of some departments.

### **3.3.6 Measurement**

A five point Likert Scale was used to allow for nonparametric inferential statistical analysis. Categorical statements were also included. The use of the Likert scale was to make it possible to measure respondents' judgements on the critical issues of concern for this research which could not be assigned categorical answers. Judgmental issues, such as satisfaction, cannot be answered categorically since individuals may experience different degrees of satisfaction.

The Likert scale has been consistently used in similar research works (Milson and Kirk-Smith, 1996). The use of this approach was, therefore, consistent with approaches used in this field.



### **3.3.7 Data Collection Methods**

#### **3.3.7.1 Questionnaire Design**

The primary data was obtained from both oral interview and mailed questionnaires. Some of the views solicited from the BCP Manager, who spearheaded the development of the plan were through oral interview. A questionnaire was also mailed to the BCP Manager to seek straightforward answers on the subject matter. Primary data obtained from the sampled staff were all through mailed questionnaire. The questionnaire was designed to enable genuine answers on the main components of the research questions. The wording of the questionnaire was made to be as simple as possible demanding only straightforward answers. Ambiguities were avoided and leading questions were simple and straightforward and not requiring respondents to delve into memory.

The Mail questionnaires were used instead of other alternatives (e.g. in-depth interviews etc) because mail questionnaires are easier, quicker and cheaper to use for data collection from primary sources.

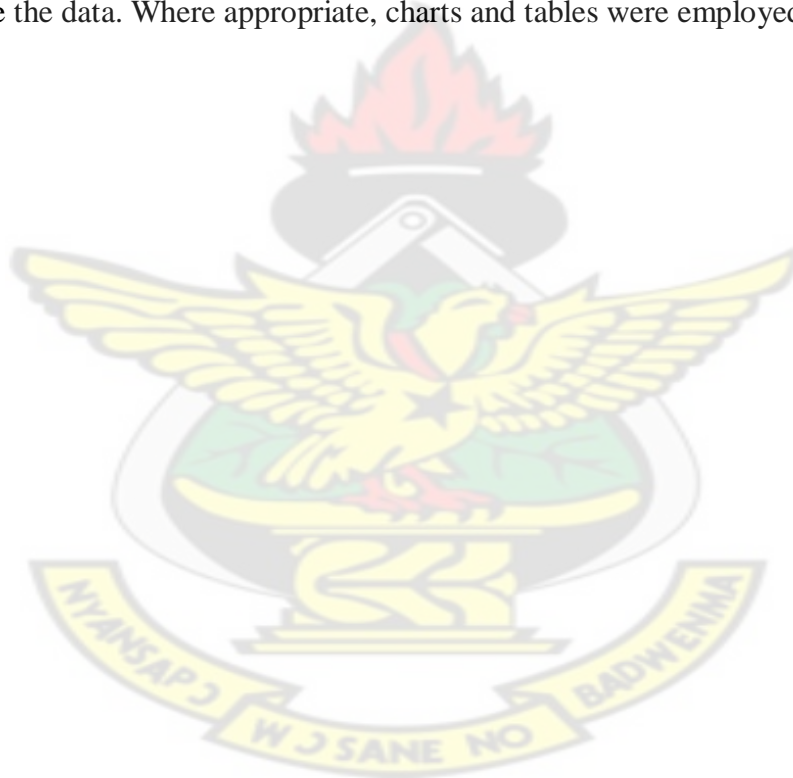
#### **3.3.7.2 Questionnaire Administration**

All questionnaires were administered by the researcher. The questionnaires were distributed to respondents through the mail (SG-SSB's Microsoft Outlook). The questionnaires were mailed because each respondent (staff) has a unique company mailing address and uses the Microsoft outlook as a form of communication within and outside the bank. This method saved time and cost and ensured that each respondent was reached thus enhancing the response rate. Follow-up mails were sent to remind respondents of the questionnaire and to find out when they could complete and return. Bank officers are busy most of the time and administering questionnaires

to them would mean finding time away from their busy routines to answer them. Taking employees off their tasks to answer the questionnaires was difficult. To remedy these difficulties, questionnaires were mailed to employees to complete and return later.

### **3.3.8 Data Analysis**

The study employed computer programmes such as Microsoft Excel and Microsoft Word to analyze the data obtained from the field. Both qualitative and quantitative techniques such as content analysis and descriptive statistics were employed to analyse the data. Where appropriate, charts and tables were employed to present data.



## **CHAPTER FOUR**

### **PRESENTATION AND ANALYSIS OF DATA**

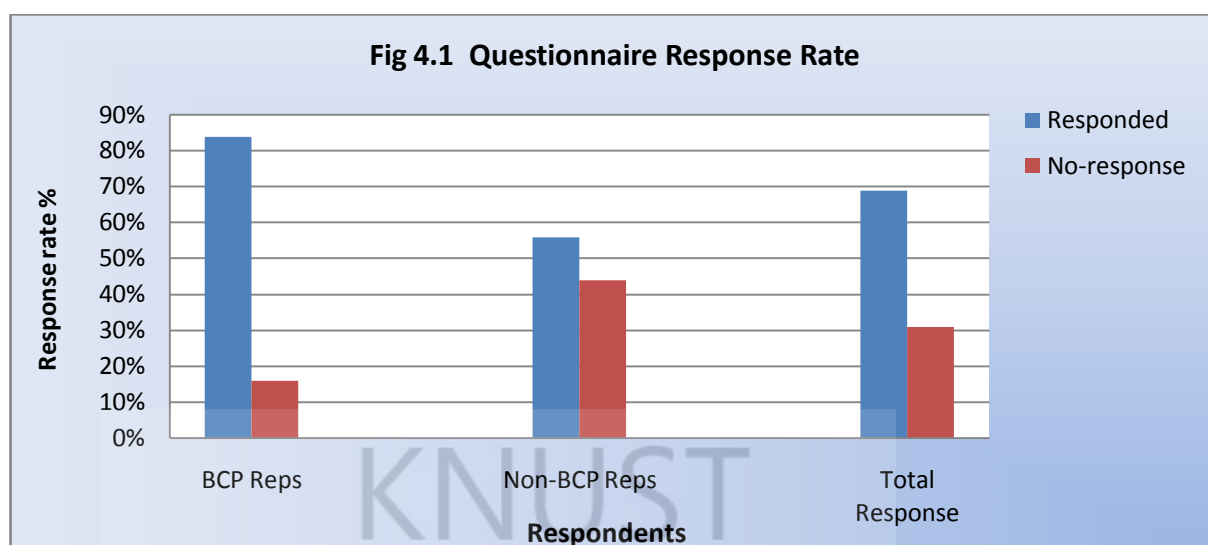
#### **4.1 INTRODUCTION**

This chapter puts forward the findings of the study, analysis and discussion. It is aimed at providing solutions to the research objectives. The study sets out to affirm the relevance of Business Continuity Plan to Financial Institutions, test the awareness of staff of the existence of a BCP and the understanding of their responsibilities if the plan is invoked in the event of a disruption. During the study, views were solicited from 3 groups; management (BCP Manager), BCP representatives of all branches/agencies and the general staff (non-BCP representatives). Study findings have been organised, presented, analysed, and discussed in two distinct sections, responses from BCP manager; and responses from BCP representatives and non-BCP representatives.

#### **4.2 RESPONSES FROM BCP REPRESENTATIVES AND GENERAL STAFF (NON-BCP REPRESENTATIVES)**

##### **4.2.1 Questionnaire Response Rate**

In all ninety nine questionnaires were sent out to employees; forty five of them are BCP representatives of the various branches/agencies and fifty four of them are general staff (non-BCP representatives) who were sampled randomly from the various branches/agencies and head office departments. However, after a follow-up, thirty eight BCP representatives out of the 45 BCP reps responded representing 84% response rate and thirty other non-BCP representatives out of 54 employees responded representing 56% response rate as shown in Fig 4.1. Overall response rate stood at 69% representing sixty eight respondents.



Source: Researcher's Field Work, 2011

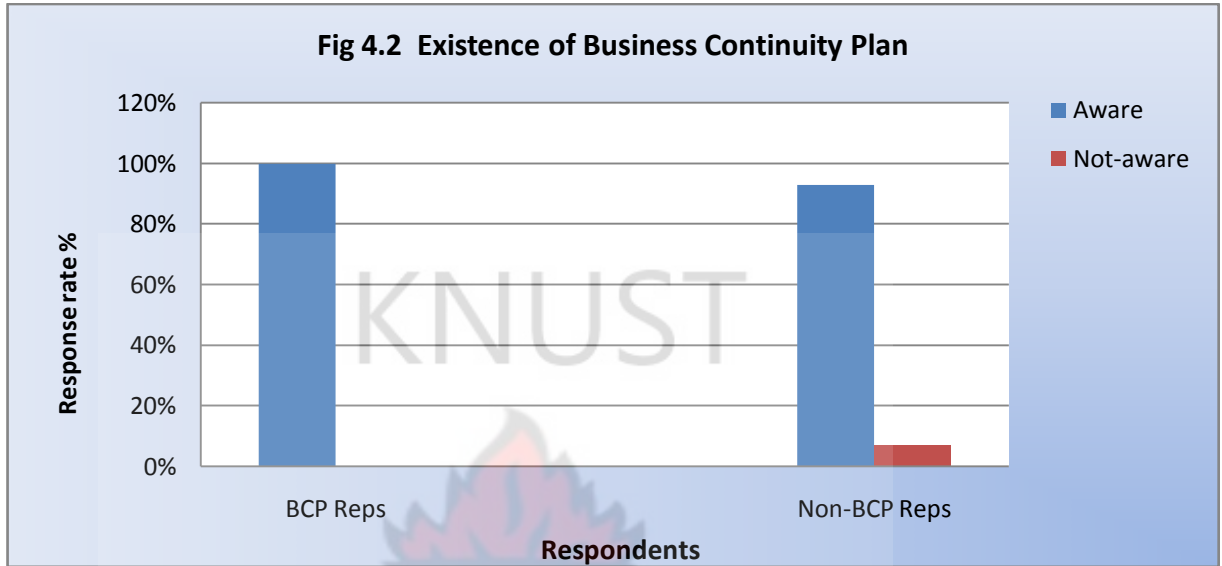
#### 4.2.2 Disruptions/Incidents in the Last 5 Years

Respondents were asked whether the bank has been disrupted by specific incidents in the last 5 years. All respondents (100%) replied NO, meaning the bank has never been disrupted by any specific incident in the last 5 years.

#### 4.2.3 Existence of Business Continuity Plan

This question sought to test the awareness of staff of the existence of a business continuity plan for the bank. All the thirty eight BCP representatives representing 100% responded Yes, meaning they are aware the bank has a BCP covering its business activities. Twenty eight other staff (non-BCP representatives) representing 93% also responded that they are aware such a plan exists. Only two staff (non-BCP representatives) responded No, meaning they are not aware the bank has a business continuity plan covering its business activities. This number represented 7% of the other staff who are non-BCP representatives. The high awareness rates of 100% and 93% depicted in Fig 4.2 for both BCP and non-BCP representatives respectively

indicate that the bank's medium for information relay is very effective. The bank achieves this through the use of the intranet and internal mail medium (Microsoft Outlook) to relay information to the general staff population.

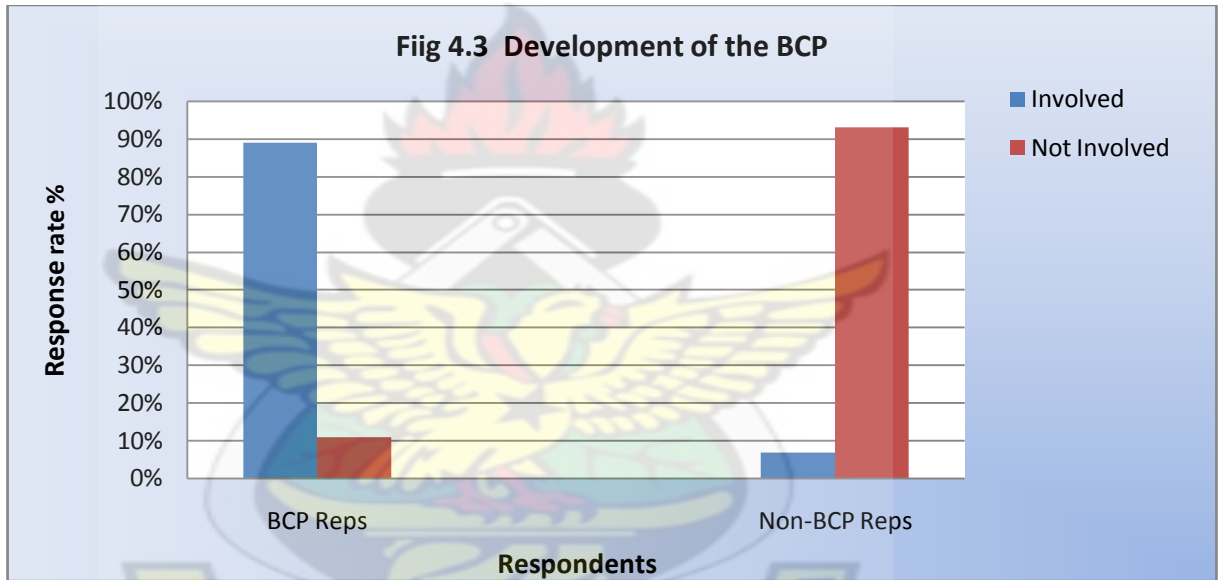


Source: Researcher's Field Work, 2011

#### 4.2.4 Development of the Business Continuity Plan

Respondents were asked whether they were involved in the development of the business continuity plan. This question sought to ascertain the level of involvement of staff in the development of the plan and the specific scenarios that were considered. Out of the thirty eight BCP reps who responded, 89% (34 BCP reps) said they were involved in the development of the plan and the remaining 11% said they were not involved. Only 2 of the 30 non-BCP respondents said they were involved in the development of the plan (these represented 7%) whilst the remaining 28 non-BCP respondents representing 93% said that they were not involved in the plan development. The 11% non involvement rate for the BCP reps indicates that the BCP development enjoyed massive participation or contribution especially from the BCP reps. The few who were not involved may be as a result of non-availability of the

reps concerned during the development period i.e. either they were on leave during the period or the branch manager contributed in their stead. Majority of the non-BCP reps however made no input in the development of the plan, thus even though the majority were aware of the existence of the plan, very few were actually involved in its development. Majority of the employees who contributed to the plan development cited scenarios such as non-access to premises, staff unavailability, IT system breakdown/failure and fire outbreaks as specific scenarios that were considered. Involvement in the development of the BCP is presented in the Fig 4.3 below.



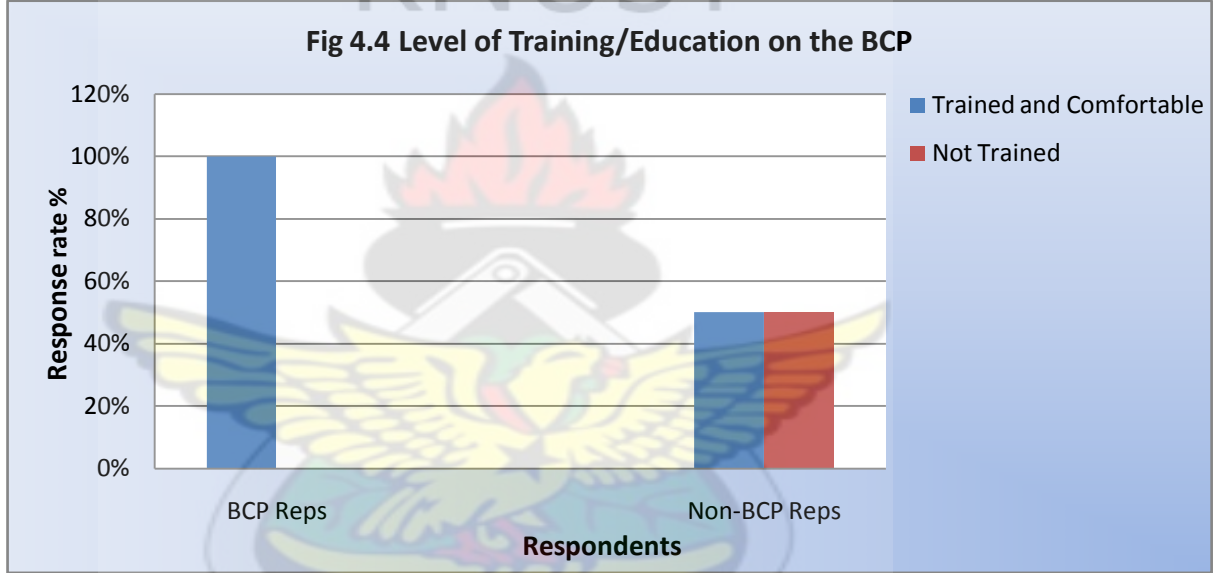
Source: Researcher’s Field Work, 2011

#### 4.2.5 Level of Training/Education on the BCP

Respondents were asked whether they have had any training or education on the business continuity plan and whether they are comfortable with the level of training or education if they have had any. Staff were also asked whether they understand their obligations in the event the plan is invoked. All the 38 BCP reps representing 100% responded that they have been trained on the BCP and are comfortable with the level of training they have received as shown in Fig 4.4. All BCP reps also



intimated that they understand their obligations in the event that the plan is invoked. There was however a split in the number of the non-BCP reps as 15 respondents representing 50% said they have been trained on the BCP and are comfortable with the level of training they have had. This number also said that they understand their obligations in the event that the plan is invoked. The remaining 50% non-BCP reps however responded that they have not had any training on the BCP thus do not understand their obligations in the event that the plan is invoked.



Source: Researcher’s Field Work, 2011

#### 4.2.6 Perceived Importance/Relevance of Business Continuity Plan

On a scale where 1 representing “of high importance”, 2 representing “important”, 3 representing “less important” and 4 representing “of no importance”, employees were asked to express their opinion on how relevant they perceive the Business Continuity Plan to financial institutions. 50% of BCP representatives think BCP is of high importance and 50% others think that BCP is important to financial institutions. Again 40% of non-BCP representatives claim BCP is of high importance whilst the remaining 60% think BCP is important to financial institutions. From the Table 4.1,

the mean value for both the BCP and non-BCP representatives is 1.5 and this implies that all respondents agree that it is relevant for financial institutions to have in place effective business continuity plans. Again lower variances and standard deviations of 1.250 and 1.118 from the mean indicate that all of the respondents understood the questions in the same way.

**Table 4.1 Perceived Relevance of BCP**

<b>Perceived Relevance of BCP</b>						
<b>Respondents</b>		<b>Freq</b>	<b>%</b>	<b><math>\hat{Y}</math></b>	<b><math>Y - \hat{Y}</math></b>	<b><math>(Y - \hat{Y})^2</math></b>
<b>BCP Reps</b>	High Importance (1)	19	50%	1	-0.5	0.25
	Important (2)	19	50%	2	0.5	0.25
	Less Important(3)	0	0%	0	-1.5	2.25
	Not Important(4)	0	0%	0	-1.5	2.25
	<b>Total</b>	<b>38</b>	<b>100%</b>	<b>1.5</b>	<b>-3</b>	<b>5</b>
		<b>Freq</b>	<b>%</b>	<b><math>\hat{Y}</math></b>	<b><math>Y - \hat{Y}</math></b>	<b><math>(Y - \hat{Y})^2</math></b>
<b>Non-BCP Reps</b>	High Importance (1)	12	40%	1	-0.5	0.25
	Important (2)	18	60%	2	0.5	0.25
	Less Important(3)	0	0%	0	-1.5	2.25
	Not Important(4)	0	0%	0	-1.5	2.25
	<b>Total</b>	<b>30</b>	<b>100%</b>	<b>1.5</b>	<b>-3</b>	<b>5</b>
<b>Mean = 1.500</b>						
<b>Variance = 1.250</b>						
<b>Standard Deviation = 1.118</b>						

Source: Researcher's Field Work, 2011

### 4.3 SUMMARY OF INTERVIEW AND RESPONSE FROM BCP MANAGER

#### 4.3.1 Introduction

The BCP manager who is the main architect behind the development of the Business Continuity plan for SG-SSB was interviewed and also made to complete some mailed questionnaire which demanded straightforward answers. Below is a summary of views and responses from the BCP manager.

#### **4.3.2 Existence, Development of BCP and Recovery from Disruptions.**

The BCP manager was asked whether the bank has encountered specific incident in the last 5 years to which he answered that the entire bank has not seen a significant or specific incident which has disrupted operations in the last five years. He however mentioned that a fire outbreak occurred at one of the bank's branches seven years ago which burnt down the entire branch building and disrupted operations at the branch. According to him the branch was able to resume operations within 7 days from surrounding branch residences until the burnt branch building was renovated 3 months later.

When he was asked whether the bank has in existence a business continuity plan which covers major operational activities of the bank, he answered that in the bank's bid to learn from such incidents, it has since developed a business continuity plan which covers major operational activities such as;

- Branch Operations
- IT services
- Finance operations
- Foreign operations
- Treasury services and
- Other critical operational activities

The BCP manager listed the following scenarios when asked to state the specific incidents which were considered in developing the plan;

- Non availability of staff
- Non access to building
- Non availability of IT systems

When asked about the major stakeholders who were involved in the development of the BCP, the manager outlined the following;

- Board of Directors
- Management
- BCP Manager
- BCP representatives of branches and departments
- Entire staff

He however stated that the BCP manager takes absolute responsibility of the BCP.

When quizzed to rate the bank's ability to recover from natural or man-made disaster or business disruption and how quickly can the bank recover from a significant/major business interruptions, he stated that for the specific scenarios which were considered in developing the BCP, the bank has a good chance to recover from natural or man-made disaster or business disruptions and it will be capable of recovering majority of its critical operations in 1 day.

#### **4.3.3 Training of Staff and Testing of BCP**

The BCP manager was asked to state whether the bank run regular exercises to train and educate staff on their responsibilities in case the plan is invoked. He stated that the bank has a program in place with the aim of educating the entire staff population within one year so that each staff will be aware of the existing plan and know what to do in case the plan is invoked in the future. He however stated that this training program started not long ago and it is still running so not everybody has been trained. He then stated that highlights of the business continuity plan, manuals and directives have been communicated and staff have access to these information through the bank's intranet.

When questioned whether the bank undertakes regular testing of the BCP and how often this happens, the manager again answered that the bank has a program in place to carry out regular simulation exercises across the entire head office buildings and branches throughout the country. These rehearsals he intimated happen every quarter in the year. The exercises he stated ranges from table top exercises through IT back up and full recovery exercise to staff coping with utility disruption exercises. These he claimed enables the plan to be revised, refined and updated before weaknesses are exposed by real disruption.

#### **4.3.4 Perceived Importance/Relevance of Business Continuity Plan**

When asked how relevant it is for the bank to have a business continuity plan, the BCP manager answered that instituting the business continuity plan was a top priority for the parent company to make sure that its entire subsidiaries worldwide have in place comprehensive and operational plan in line with the group's policy. Notwithstanding this the BCP manager stated that it is still of high importance for financial institutions to develop effective business continuity plans not only because of the increasing threats but in order to meet the rising competition and high demands by customers and many more.

The manager further stated that the bank has a dedicated budget for the BCP because of the importance it places on the need to have the plan.

#### **4.3.5 Perception of Threats**

The BCP manager was quizzed on his perception on the probability of occurrence of particular threats in the bank. As shown in Table 4.2, computer virus; fraud and corruption; loss of electricity/power; and fire all have the highest chance of 100% of

occurring in the bank. Loss of IT; loss of telecommunication; theft of documents and equipment; and loss of water and sewerage also have high probabilities (75%) of occurring. Terrorist attack and extreme weather have the lowest chance of 25% to occur in the bank.

A similar question examines the manager's perception on particular threats, asking what disruptions would have a significant impact on cost and revenue of the bank. As shown in the Fig 4.5, loss of IT; loss of access to site; loss of telecommunication; loss of electricity/power; industrial action; terrorist attack; and computer virus all have common concerns and will have the highest impact (100%) on the bank's cost and revenue should they occur. Loss of people; damage to corporate image/reputation/brand; loss of key skills; employee health and safety incident; environmental incident; and fire will also have a high impact of 75% on the bank's cost and revenue.

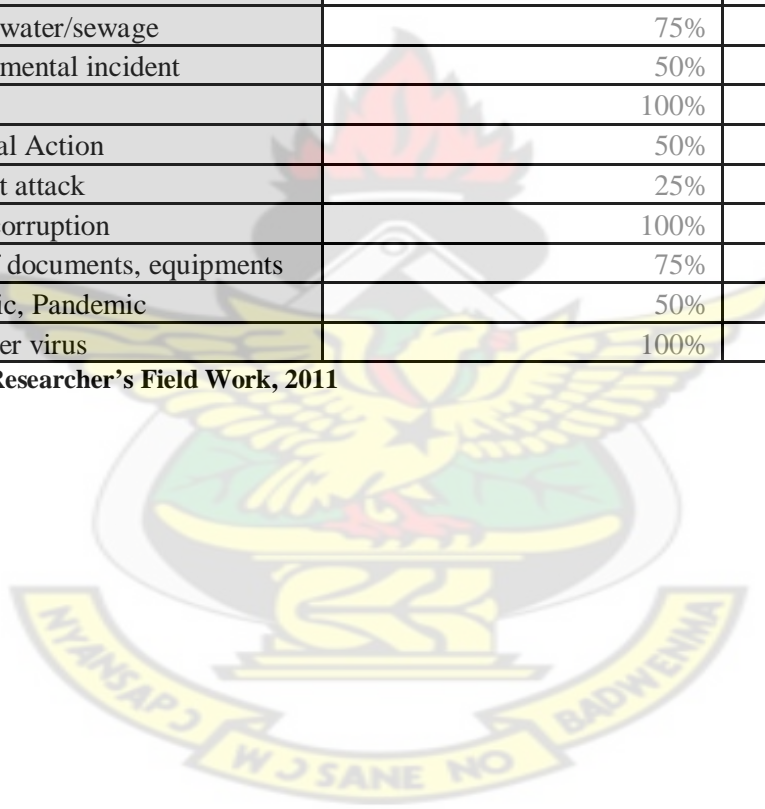
Despite the reality of their substantial impact on organisations across the country, the manager ranked extreme weather and loss of water/sewerage as threats that will have the least impact of the company's cost and revenue.

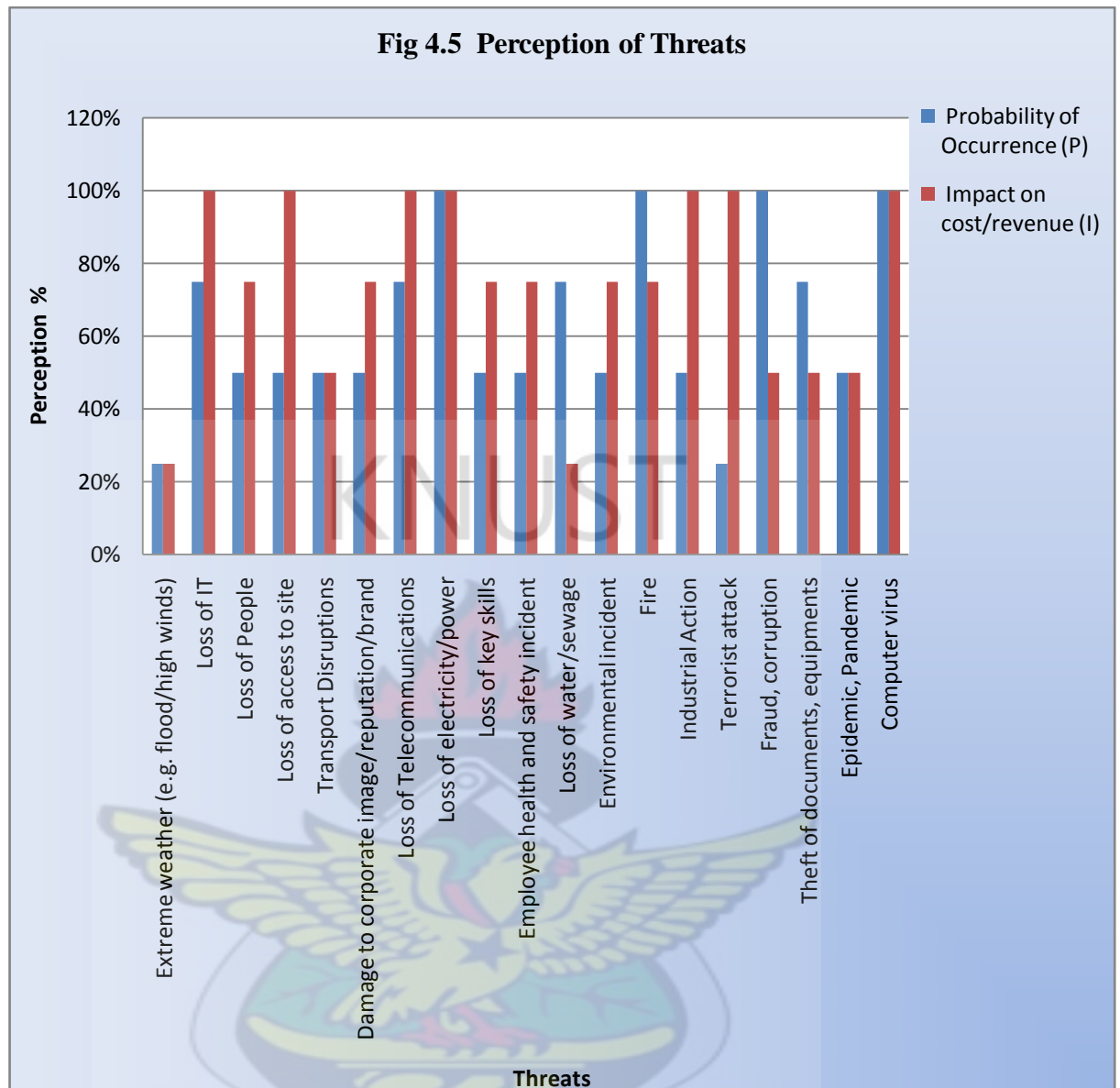


**Table 4.2 Perception of Threats**

Threats	Probability of Occurrence (P)	Impact on cost/revenue (I)
Extreme weather (e.g. flood/high winds)	25%	25%
Loss of IT	75%	100%
Loss of People	50%	75%
Loss of access to site	50%	100%
Transport Disruptions	50%	50%
Damage to corporate image/reputation/brand	50%	75%
Loss of Telecommunications	75%	100%
Loss of electricity/power	100%	100%
Loss of key skills	50%	75%
Employee health and safety incident	50%	75%
Loss of water/sewage	75%	25%
Environmental incident	50%	75%
Fire	100%	75%
Industrial Action	50%	100%
Terrorist attack	25%	100%
Fraud, corruption	100%	50%
Theft of documents, equipments	75%	50%
Epidemic, Pandemic	50%	50%
Computer virus	100%	100%

Source: Researcher's Field Work, 2011





Source: Researcher's Field Work, 2011

#### 4.4 SUMMARY OF FINDINGS

This chapter presented the research findings which are summarised as follows;

- SG-SSB Limited has not encountered major disruptions in the last five years.

However a fire outbreak occurred in one of the bank's branches seven years ago which burnt down the entire branch building and disrupted operations at

the branch. The branch was however able to resume operations within 7 days from adjacent bank properties.

- SG-SSB has developed a Business Continuity plan covering its major or critical operations like, Branch Operations; IT services; Finance operations; Foreign operations; Treasury services and other critical operational activities. The plan was also developed to cover specific scenarios which were; Non availability of staff; Non access to building; Non availability of IT systems.
- The main stakeholders involved in the development of the business continuity plan were, The Board of Directors; Senior Management; BCP manager; and staff. Staff involvement was however minimal and mainly limited to the BCP representatives at the branches and departments. The BCP manager carries the optimum responsibility to ensure the continuous and effective running of the plan.
- The bank has a good chance to recover from natural or man-made disaster or business disruptions and is will be capable to recover in 1 day with respect to the specific scenarios which were considered in developing the plan.
- The Bank has instituted a training program to train the entire staff population to be on top of their responsibilities in the event where the plan is invoked. Manuals and directives are also made available to staff through the bank's intranet. However not every staff has benefited from the training program. All BCP representatives have been trained and are comfortable with their level of training. Only half of the non-BCP representatives claimed to have had some training and are comfortable with the training received. The other half of the non-BCP representatives have not had any training at all.

- The bank also has in place a program to run various simulation exercises ranging from table top exercises through IT back up and full recovery exercises to staff coping with utility disruption exercises.
- Majority of respondents agree having a business continuity plan should be of high importance and priority to financial institutions. SG-SSB places high importance on relevance of BCP to financial institutions not only to meet its parent company's policy and requirements but also in meeting the increasing threats, rising competition and high demands by customers etc.



## **CHAPTER FIVE**

### **DISCUSSIONS, CONCLUSION AND RECOMMENDATIONS**

#### **5.1 INTRODUCTION**

This chapter includes: Discussions, conclusions, recommendations, limitations and future work. Discussions attempt to relate research findings to theory. Conclusions are the researcher's opinions depending on the outcome from the data analyzed as per the objectives of the study. Recommendations are the way forward resulting from conclusions and are very vital for policy making. Limitations are set to explain the restrictions of the study. Further work gives an area of importance that the researcher left unexplored in relation to the ongoing study.

#### **5.2 DISCUSSIONS**

The study points to the fact that an organisation's board of directors and senior management should be very much involved in the development of the company's business continuity plan. As highlighted in one of the five high level principles of business continuity findings by the Joint Forum-Basel Committee on Banking Supervision, an organisation's board and senior management are responsible for managing its business continuity effectively and for developing and endorsing appropriate policies to promote resilience to, and continuity in the event of operational disruptions. They should recognise that outsourcing a business operation does not transfer the associated business continuity management responsibilities to the service provider. The board and senior management should create and promote an organisational culture that places a high priority on business continuity. This

message should be reinforced by providing sufficient financial and human resources to implement and support the organisation's approach to business continuity management.

The study also indicated that financial institutions should undertake regular testing of the BCP in order for the plan to be revised, refined and updated before weaknesses are exposed by real disruption. Testing of the ability to recover critical operations as intended is an essential component of effective business continuity management. Such testing should be conducted periodically, with the scope and frequency determined by the criticality of the applications and business functions, the organisation's role in broader market operations, and material changes in the organisation's business or external environment. In addition, such testing should identify the need to modify the business continuity plan and other aspects of an organisation's business continuity management in response to changes in its business, responsibilities, systems, software, hardware, personnel, or facilities or the external environment.

By the majority acclamation the study affirmed that it highly relevant for financial institutions to have in place an effective business continuity plan. Rising competition and higher demands of customers, such as the expectation of 24/7 availability of (digitalized) services makes it necessary for organizations to pay extra attention to their continuity assurance. Threats and visibility of threats and their consequences that endanger the continuity of a business are increasing. These and may other reasons underscore the relevance business continuity to financial institutions.

Again the research work presented that the business continuity plan should cover financial institutions major or critical operations like, Branch Operations; IT services; Finance operations; Foreign operations; Treasury services and other critical



operational activities. The BCP should also be prepared based on specific or major operational disruptions such as; Non availability of staff; Non access to building; Non availability of IT systems etc. The extent to which a financial industry participant prepares to recover from a major operational disruption should be based on its unique characteristics and risk profile. Because access to the resources needed for the full recovery of its operations may be limited during a major operational disruption, a financial industry participant should identify through a business impact analysis those business functions and operations that are to be recovered on a priority basis and establish appropriate recovery objectives for those operations.

### **5.3 CONCLUSION**

In order to achieve the main objective, the study focussed on specific objectives, the first one was to find out whether SG-SSB has in place a business continuity plan which covers its major operations and which specific scenarios the plan was based on. It is concluded that the bank indeed has developed a business continuity plan which covers its major operations. Three critical scenarios or incidents formed the basis for the development of the plan. However this plan is limited to these three incidents and may not suffice effectively as contingency plan for other equally critical and potential incidents or disruptions in the future.

A second specific objective was to find out whether the bank undertakes periodic testing of the plan to review and update the plan and whether there is a periodic training of staff so that they know about the plan and their responsibilities. It is concluded that the bank undertakes various exercises in order to test, review and update the plan. It is also concluded that even though the bank undertakes training programs for staff, not every staff has undergone the training and therefore not every

staff understands their obligations or responsibilities should the plan be invoked in the event of a disruption.

Another specific objective was to find out the stakeholders who took part in the development of the plan. In conclusion, the bank's board of directors, senior management, BCP manager and staff were involved in the development of the plan. However not every staff was involved; only the BCP representatives and few other non-BCP representatives were involved in the development of the plan. Majority of staff are also aware of the existence of the business continuity plan.

The main objective of the study was to affirm the relevance of business continuity plan to financial institutions. From the responses of the field survey and interview, it is encouraging to note and conclude that majority of the staff agree that it is of high importance for financial institutions to have business continuity plan that covers their major operations critical to the survival of the business in case of disruptions. SG-SSB Limited places high importance on the plan not only to meet a policy requirement by its parent company, but as a result of several other reasons such as rising competitions, demands by customers and many more. As a result of this, the bank has a dedicated budget that ensures the sustainability of the plan. Various theories reviewed also underscore the relevance of a well designed, implemented and tested business continuity plan to organisations and financial institutions especially against financial perils.

## 5.4 RECOMMENDATIONS

The researcher strongly recommends that;

- Financial institutions should develop a robust, comprehensive and proportionate business continuity plan that covers majority of critical incidents or disruption scenarios in order to develop resilience in parts of their business that are central to the continuity of operations.
- The development of the Business Continuity Plan should be a cross-functional project with all hands-on-deck approach, not only a few senior management and staff. The Human Resources Department will be an important stakeholder in this exercise in identifying and harnessing the skill of staff to ensure that a comprehensive plan is development.
- It is imperative for financial institutions to inform their staff through their various communication channels of the policies, standards and practises of existing business continuity plans and train their entire staff and engaged them in refresher courses periodically in order for them to be on top of their responsibilities should the plan ever be invoked.
- Senior management must therefore take ultimate responsibility for the BCP, ensuring that plans are properly developed, maintained and well communicated not only to employees but to shareholders and customers as well.
- It is highly important for financial institutions to rehearse their business continuity plans periodically to expose flaws and enhance their effectiveness, at least annually and these rehearsals should encompass all the processes and people involved in the BCP.

## **5.5 LIMITATIONS**

In spite of the contribution this research has made to affirm the relevance of BCP to financial institutions in general, there are limitations associated with the research we wish to highlight. First the sample is based on 100 respondents. This is woefully inadequate to generalise findings for the entire financial institutions. The sample size was chosen due to limited resources and time constraints especially since the period allotted for the thesis work was limited. A major difficulty too was with tracing and getting an interview with the BCP manager and getting him to also complete the questionnaires which formed the basis of the analysis. This emerged since he is very busy with large commitments and responsibilities. This therefore limited the number of questions posed to him as a result of his large commitments and responsibilities. Moreover he was not forthcoming with detailed answers which could have enriched the analysis. Lastly, the study was mainly limited to business continuity plan for and responses from staff of SG-SSB, this could have been extended to cover other financial institutions if not for time constraint and reluctance of banks releasing confidential or sensitive information.

## **5.6 FUTURE WORK**

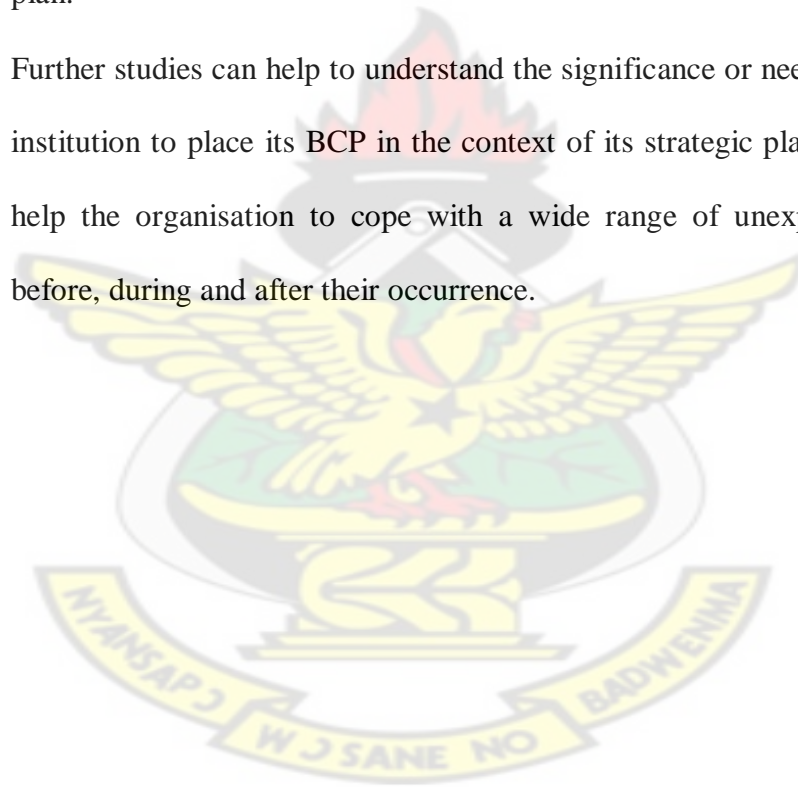
Although this research has contributed to the acceptance of the relevance of business continuity plan to financial institutions and the need to undertake periodic training of staff and regular testing of the plan, it has prompted the need for further research.

Future research should focus on a number of issues:

- This research focussed on one financial institution in order to affirm the relevance of business continuity plan for financial institutions, the stakeholders involved in the preparation of the plan, the awareness of staff of

the existence of the BCP and a test of the understanding of their obligations. Further studies should focus on more than one financial institution in order to have broad views that cut across the entire financial industry.

- Future research should evaluate the level of business continuity planning or management within a financial institution in order to identify the key factors involved in the BCP which will ensure resilience in the event of disruption. The researcher can then develop a cost effective model for the evaluation of an institution's BCP which can give hints on which areas to improve upon the plan.
- Further studies can help to understand the significance or need for a financial institution to place its BCP in the context of its strategic planning. This will help the organisation to cope with a wide range of unexpected incidents before, during and after their occurrence.



## Bibliography

Bank of Japan (2003) Business continuity planning at financial institutions, Available from: <http://www.boj.or.jp/en/set/03/fsk0307a.htm>. [Accessed January 15, 2011]

BCI (2011) *Business Guide to Continuity Management*, Available from: [www.bci.org](http://www.bci.org), [Accessed January 15, 2011]

BCI (2008), *Glossary of General Business Continuity Management Terms*, The Business Continuity Institute. Available from: <http://www.thebci.org/Glossary.pdf>, [Obtained May 7, 2008]

British Standards (2008a), BS25999. Available from: <http://www.bs25999.com/BS25999-Part-1/Business-Continuity-Glossary.html>, [Obtained April, 14 2008]

CCTA (1995) *A guide to business continuity management*, CCTA.

CCTA (1995) *An introduction to business continuity management*, CCTA.

Continuity Central (2008), Available from: <http://www.continuitycentral.com/newtobusinesscontinuity.htm>, [Obtained May 9, 2008]

Cummings, J. (2005). *Nurturing a Culture of Continuity*. Network World, Vol. 20, Issue42, pp. S4-S6.

Daniel Fairley, J.D. and David A. Bjork (2006) *Boardroom Briefing. Vol.3, No.1, A publication of Directors & Boards magazine*. David Shaw. GRID Media LLC Available from: <http://www.directorsandboards.com/BoardroomBriefing6.pdf> [Accessed March 15, 2011]

Gartner (2002). Press release. *Gartner Says That Less Than 25 percent of Global* Available from: [http://www3.gartner.com/5\\_about/press\\_releases/2002\\_10/pr20021008a.jsp](http://www3.gartner.com/5_about/press_releases/2002_10/pr20021008a.jsp) [Accessed October 8, 2004]

Gibb, F. and Buchanan, S. (2006). *A Framework for Business Continuity Management*. International Journal of Information Management, Vol. 26, Issue 2, pp. 128-141.



Gibson, D. (2000), Firestone's failed recalls, 1978 and 2000: *A public relations explanation*, *Public Relations Quarterly*, Vol. 45, No.4, pp 10-13.

Gibson, C., Britton, N., Love, G., Porter, N. & Fernandez, E. (2004), *Handbook: Business Continuity Management*, HB 221:2004.

Industrial Safety and Hygiene News (ISHN) Online. *NFPA 1600 to Become the National Preparedness Standard?* Available from:  
[http://www.ishn.com/CDA/ArticleInformation/news/news\\_item/0,2169,123889,00.html](http://www.ishn.com/CDA/ArticleInformation/news/news_item/0,2169,123889,00.html) [Accessed April 30, 2004]

Koch, R. (2004). *Best Practices in Business Continuity*. Communications News, Vol. 41, part 11, pp. 24-25.

Leegwater, D., & Ploeg, J. (2005), *Business Continuity Management* sterk gebaat bij procesdenken, *Business Process Magazine*, Vol.3, pp 27-30

Leegwater, D. & Reiniers, C. (2005), *Business Continuity Management* – Methodiek en lessen vanuit de praktijk, *Jaarboek IT beheer en Informatiebeveiliging*

Mitroff, Ian I., Pauchant, Thierry, C. (1992) *Transforming the Crisis-Prone Organization*. Jossey-Bass, Inc. San Francisco, CA.

Mitroff, Ian. I. (2001) *Managing Crises Before They Happen: What Every Executive and Manager Needs to Know About Crisis Management*. Amaco. New York, NY. 2001.

Moore P. (1995), 'Critical Elements of a Disaster Recovery and Business/Service Continuity Plan' *Facilities*, Vol. 13 Iss: 9/10, pp.22 – 27

National Fire Protection Association. NFPA 1600 (2004) *Standard on Disaster/Emergency Management and Business Continuity Programs*. 2004 Edition. Quincy, MA. 2004.

NFPA 1600 (2007), *Standard on Disaster/Emergency Management and Business Continuity fs*. 2007 Edition, National Fire Protection Association.

Noakes-Fry, N., & Diamond, T. (2001), *Business Continuity Planning and Management: Perspective*, Gartner Research

Oud, E.J. (2000), *Business Continuity Management; meer dan Contingency Planning*, IB jaarboek

Reason Magazine (March 2007), FM Global, p.18.

Scheffel,(2004) *Het doel, de weg en de rugzak; een gids voor praktisch ICT service management*,Verdonck, Klooster & Associates, van Haren Publishing, 2004

Smit, N. (2005). *Business Continuity Management: A Maturity Model*. Master's Thesis, Erasmus University, Rotterdam.

Snedaker, S., (2007) *Business Continuity and Disaster Recovery Planning for IT Professionals*, Syngress Publication, Inc.

Spring Singapore,(N.D) *Fact sheet on business continuity management*, Available from: [http://www.spring.gov.sg/portal/products/nat\\_certification/bcm/bcm.html](http://www.spring.gov.sg/portal/products/nat_certification/bcm/bcm.html) [Accessed January 15, 2011]

Shaw, G. L., (N.D) *Business Crisis and Continuity Management*, Available from: <http://www.gwu.edu/~icdr/publications/ShawTextbook011105.pdf> [Accessed January 15, 2011]

Wikipedia (2008a), Available from: [http://en.wikipedia.org/wiki/Risk\\_management](http://en.wikipedia.org/wiki/Risk_management), [Obtained May 9, 2008]

Wikipedia (2008b), Available from: [http://en.wikipedia.org/wiki/Business\\_continuity](http://en.wikipedia.org/wiki/Business_continuity). [Obtained May 9, 2008]

Wheatman, Vic, Scott, Donna, Witty, Roberta (2001). *Aftermath: Business Continuity Planning*. Gartner Top View. AV-14-5138. Available from: <http://www.gartner.com> [September 21, 2001]

Woodman, P & Hutchings, P. (2010), *Disruption & Resilience, Business Continuity Management Survey*, Chartered Management Institute (CMI)

Yankee Group (2001), September 11, 2001: *Infrastructure Impacts, Implications, and Recommendations*, Yankee Group Special Report, September 2001

## Appendix A - Questionnaire

### 1. QUESTIONNAIRE - STAFF

#### *Business Continuity for Financial Institutions – A case study of SG-SSB Limited*

##### Introduction

The questionnaire is to enable the student of the KNUST conduct a study into the relevance of Business Continuity for Financial Institutions with particular reference to how SG-SSB Limited is managing its Business Continuity.

Note: Results from this study will be used primarily for research purposes and your responses status will be treated confidentially. Your kind co-operation will be very much appreciated.

1. Please state your department/Branch.

.....

2. Has the company (SG-SSB Limited) ever been disrupted by a specific incident(s) in the last 5 years? Yes ☐ No ☐

3. If yes, which major disruption has the Bank encountered in the last 5 years?

i.....

ii.....

iii.....

4. Are you aware the Bank has a Business Continuity Plan (BCP) covering its business activities? Yes ☐ No ☐

5. Does your department have a BCP representative? Yes ☐ No ☐

6. If yes, are you the representative? Yes ☐ No ☐

7. Were you involved in the development of the BCP? Yes ☐ No ☐

8. If Yes, which specific scenarios/incidents were considered in developing the BCP?

i.....

ii.....

iii.....

iv.....

v.....

9. Have you had any training/education on the BCP? Yes ☐ No ☐

10. If Yes, are you comfortable with the level of training/preparation. Yes ☐ No ☐

11. If Yes, do you understand your obligations in the event the plan is invoked?

Yes ☐ No ☐

**On a scale where 1="of high importance" and 4="of no importance".**

12. In your opinion, how relevant is Business Continuity to financial institutions?

1      2      3      4

Thank you very much

## 2. QUESTIONNAIRE – BCP MANAGER

1. Has the company (SG-SSB Limited) ever been disrupted by a specific incident in the last 5 years? Yes ☐ No ☐

2. If yes, which major disruption has the Bank encountered in the last 5 years?

i.....

ii.....

iii.....

3. Does the Bank have a Business Continuity Plan (BCP) covering its business activities? Yes ☐ No ☐

4. Does the BCP cover major operational activities of the Bank which are critical to the survival of the company in the event of a disruption? Yes ☐ No ☐

5. If yes, what main operational activities does the BCP cover?

i.....

ii.....

iii.....

iv.....

v.....

6. Which specific scenarios/incidents did you consider in developing the BCP?

i.....

ii.....

iii.....

7. How do you rate the Bank's ability to recover from natural or man-made disaster or business interruption?

i) Excellent    ii) Good    iii) Fair    iv) Poor    v) Other.....

8. How quickly do you estimate the bank can recover from a significant or major business interruption?

i) Minutes    ii) Hours    iii) Days    iv) Weeks    v) Months

**(On a scale where 1="of high importance" and 4="of no importance").**

9. In your opinion, how relevant is Business Continuity to financial institutions?

1    2    3    4

10. On a rating of 1 – 4, kindly state the Probability of occurrence and Impact of the following threats/disruptions on cost and revenue of the bank?

Threats	Probability (P)	Impact (I)
	1-4**	1-4**
Extreme weather (e.g. flood/high winds)		
Loss of IT		
Loss of People		
Loss of access to site		
Transport Disruptions		
Damage to corporate image/reputation/brand		
Loss of Telecommunications		
Loss of electricity/power		
Loss of key skills		
Employee health and safety incident		
Loss of water/sewage		
Environmental incident		
Fire		
Industrial Action		
Terrorist attack		
Fraud, corruption		
Theft of documents, equipments		
Epidemic, Pandemic		
Computer virus		

\*\*The analysis is based on a synopsis rating system between 1 to 4 where:

1 = low

2 = average

3 = high

4 = very high

An activity with a high rating generates more income, uses more resources, is more sensible to risks etc. than an activity with a low rating.

11. Do you run regular exercises to train and educate staff on their responsibilities in case the plan is invoked in the event of a disruption? Yes ☐ No ☐

12. Do you undertake regular rehearsals/testing of the BCP in order to refine, revise and update the plan? Yes ☐ No ☐

13. If yes, how often to you undertake the rehearsal/testing of the BCP?

i) Monthly                      ii) Quarterly                      iii) Half Yearly                      iv) Yearly

v) Other.....

14. If No, why?

.....  
.....

15. Is there a dedicated budget for the BCP? Yes ☐ No ☐

16. Who were the major stakeholders in the development of the BCP? Please list.

.....  
.....

17. Who takes responsibility of the existing BCP?

i) Board of Directors                      ii) Managing Director                      iii) General Managers

iv) Heads of Department                      v) BCP Manager                      vi) Staff

vii) Other.....

Thank you very much



# KNUST

