BUSSINESS CONTINUITY MANAGEMENT SYSTEM AT KENYA BUREAU OF STANDARDS

BY

PERSILA AKINYI OKUNA

A Research Project Submitted in Partial Fulfillment of the Requirement for the Award of the Degree of Master of Business Administration, School of Business, University of Nairobi

OCTOBER 2014

DECLARATION

I declare that this Project is my original work and has not been presented in any other university for academic purposes.

Signature……. **Date**……

PERSILA AKINYI OKUNA

REG. NO. D61/68344/2011

This project has been submitted with my approval as the university supervisor.

Signature……. **Date**…….……...

MRS. ZIPPORAH KIRUTHU

DEPARTMENT OF MANAGEMENT SCIENCE

SCHOOL OF BUSINESS

UNIVERSITY OF NAIROBI

ACKNOWLEDGEMENTS

I am deeply indebted to my supervisor, Mrs. Zipporah Kiruthu, who guided and encouraged me throughout this study. Thank you very much and may God bless you. I also would like to thank my moderator Mr. Tom Kongere and the respondents and all those who participated in this research and the compilation of this report.

My heartfelt appreciation goes to my husband Bjoern and my children Bradley, Prudence, Candy and Curtney, for keeping me going. They were a big motivation behind my MBA, a blessing and a great source of strength and encouragement. Special thanks goes to my mother Isdora Okuna for her endless prayers and emotional support. I deeply appreciate all of you and may God continue blessing you.

Finally, I would like to acknowledge the support and encouragement I received from my many friends and from my colleagues at Kenya Bureau of Standards. They have been a blessing and an enrichment to my academic life.

May God bless you all abundantly!

DEDICATION

I dedicate this project to my husband, Dr. A. Bjoern Carle, for his full support, everyday encouragement and understanding throughout the period I have been pursuing this course. May God bless you abundantly, my love.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

EXECUTIVE SUMMARY

Societal Security - Business Continuity Management System (ISO 22301:2012) is the world's first international standard for Business Continuity Management, developed by the International Organization for Standardization (ISO) to specify requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise(ISO 22301:2012). International standards are considered to be the main drivers for many aspects of Business Continuity Management (BCM) practice (Ihab, Sawalha, & Anchor, 2012). The Kenya Bureau of Standards (KEBS), the National Standards Body, adopted this ISO standard as a Kenyan Standard to enable organizations in Kenya to assess their ability for business continuity after an incident. No study in Kenya has covered a holistic BCMS whose performance depends on the implementation of the requirements of the BCMS. The study focuses on three requirements which include leadership, context of organization and operational requirements. The general objective of the study was to evaluate the implementation of BCMS at KEBS. The research design employed in this study is descriptive in nature. The study focused on KEBS which represents a huge government corporation in terms of revenue and strategic importance based on standardization (in this case, management system standard). This study targeted 60 staff members at KEBS headquarters including the directorate, heads of departments, officers and non-technical staff. Primary data was collected using self-administered questionnaires. The data collected is presented through use of summarized percentages, proportions and tabulations. The study reveals systems in place at KEBS to address Business Continuity (BC), top management commitment to the implementation of BCMS at KEBS and the operational requirements implemented at KEBS. The study concludes that the Kenya Bureau of Standards has partially implemented BCMS. Major challenges in full implementation of a BCMS include full top management commitment, and the absence of government interference and bureaucracy. The study recognizes that IT outages, data breach, cyber-attacks and business ethics incidents are major threats to BC at KEBS and recommends improvement on communication/ awareness of BCMS requirements to all staff and accommodation in regulations of the need for BCMS in Government organizations.

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

Disasters are a global threat to all businesses. Westgate Mall in Kenya was attacked on 21st September 2013. The Mpeketoni terrorist attack in Lamu in June 2014, flood occurrences in Budalangi, Western Kenya, disease outbreaks, and the landslide in Muranga are just a few disaster cases in Kenya. The government of Kenya has lost resources and income from these disasters. At the organizational level, such disasters are disruptive and may affect the smooth running of businesses. According to (Pearson & Woodman, 2012), besides natural disasters and terrorist attacks, other events affect business continuity such as strikes/riots, international, social and political unrest and technological outages, e.g. the failure of Blackberry servers in October 2011, among others. Other threats to business continuity include, according to (Pearson & Woodman, 2012), loss of employees, loss of site access, loss of IT, loss of key skills, employee health and safety incidences, supply chain disruptions, damage to corporate image/brand, transport disruptions, fire, environmental incident, pressure group protest, loss of water/sewerage/electricity/gas supplies, and others. This is an indication that all organizations, including public organizations, are prone to disasters and disruptions of any nature in Kenya as well.

According to (Ethne', Dominic, & Brahim, 2003), the destruction of the World Trade Center (WTC) in New York City, USA in 2001 highlighted the need for Business Continuity Management (BCM). Major public companies in the USA also described climate-related risks and costs, among them Chevron Corporation. After hurricane Katrina struck the US Gulf coast on 29th August 2005 and hurricane Rita three weeks later, the Pascagoula refinery processed less crude oil and gasoline resulting in a $1.4 billion negative impact in the second half of the year for Chevron (CDP, 2014). The H1N1 influenza (Swine Flu) pandemic in 2009 left around 6000 people dead, between April to October 2009, according to the (CDC, 2011). These and many other incidences call for the implementation of a robust BCMS. According to a report by the (Resilience Development Initiative, 2014), the Indonesian government committed to reduce Green House Gas emmissions by 26% after the 2004 Tsunami event, since some of the other environmental disasters that struck this country had been triggered by climate change. Indonesia's disaster policy has also experienced rapid development. A continent-by-continent survey carried out by the Business Continuity

Institute, (Business Continuity Institute in association with BSI, 2014) revealed that overall, 44% of their respondents currently use ISO 22301 as a framework for their Business Continuity program and that in sub-Saharan Africa, around 65% of respondents were more likely to use ISO as a framework for BCM.

1.1.1 Business Continuity Management System

The Business Continuity Management System (BCMS) standard ISO 22301:2012 is the world's first international standard for Business Continuity Management, developed by the International Organization for Standardization (ISO) to specify requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise. This management system (BCMS) is generic and can be applied in any type and size of organization. It covers organizational structure, policies, planning activities, responsibilities, procedures, processes and resources (ISO 22301).

Business continuity (BC) is the capability of organizations to continue the delivery of products or services at acceptable, predefined levels following a disruptive incident. Business Continuity Management System (BCMS) is an operational strategy in the discipline of operations management. It has inputs in terms of interested parties and business continuity requirements, processes that include the establishment, implementation, operation, monitoring and review, maintenance and improvement of policy, objectives, targets, controls, processes and procedures and output as a managed business continuity.

Performance, according to definitions in ISO 22301:2012, is a measurable result relating to qualitative and quantitative findings; and can relate also to the management of activities, processes, products, systems or organizations. The performance of BCMS depends on the implementation of the requirements of the BCMS which include the context of an organization, leadership commitment, planning, support, operational requirements, performance evaluation and improvement. For the sake of this study, the focus was on leadership, context of organization and operational requirements. These three parameters were chosen as they are prerequisites for the implementation of a BCMS. The leadership oversees the implementation,

development and testing of Business Continuity Planning (BCP) (WauchopeMC, 2011). The context of the organization is key in understanding both external and internal issues relevant to an organization's purpose, which will affect its BCMS including the scope of implementation. Operational requirements touch on the issues regarding planning, implementation and control of processes, which are needed to meet BCMS requirements. The three requirements are therefore of paramount importance to implementation of BCMS.

1.1.2 Implementation of BCMS

The implementation of BCMS requires an organization to have in place the requirements stated in BCMS, which include context of an organization, leadership commitment, planning, support, operational requirements, performance evaluation and improvement.

Leadership establishes the organization's policy, provides resources and assigns responsibilities. Context of organization describes the policy, objectives, scope of BCMS and expectations of stakeholders. Planning describes actions required to establish strategic objectives and guiding principles for the BCMS as a whole, which set the context of business impact analysis, risk assessment and business continuity strategy. The plan should be based on continuity objectives that have been set by the organization and communicated throughout the organization. Under support, resources are key in the implementation of a BCMS, and the provision of resources shall be in a timely and efficient manner, in the form of finance and funding, personnel and personnel-related resources including training, exercising, communication with interested parties, ICT, facilities including work location and infrastructure, management and control of all forms of documented information and communication with interested parties.

Operational requirements include business impact analysis, risk assessment, BC strategy, BC procedures and exercise and testing of the BC procedures. Performance evaluation of the BCM against established standards enables organisations to ensure that they meet good practice and are in a position to effectively cope with disruption (Pearson & Woodman, 2012). A BCMS needs on-going maintenance and improvements through the identification of non-conformities, development of a

corrective action plan and continual improvement of the BCMS with an aim of meeting its objectives.

1.1.3 Kenya Bureau of Standards

Kenya Bureau of Standards (KEBS) is a state corporation/parastatal established in 1974 through an Act of Parliament, the Standards Act Cap 496 Laws of Kenya, to promote standardization in commerce and industry by providing testing and calibration facilities, assisting in the implementation and practical application of standards and maintenance and dissemination of the International System of Units (SI). It is also mandated to undertake educational work in standardization and control the use of standardization marks. Product and system certification is therefore one of its key roles. KEBS is a National Standards Body (NSB) and therefore represents Kenya in standardization work as a member of ISO, East African Community (EAC), African Organization for Standardization (ARSO), and International Electro-technical Commission (IEC). KEBS also serves as National Focal Point for the CODEX Alimentarius Commission and is a National Inquiry Point for the World Trade Organization (WTO). It is therefore the eye of the country when it comes to national, regional and international standardization. KEBS is expected to be on the frontline when it comes to implementing standards, and for that reason, it took an initiative to adopt ISO 22301:2012, the BCMS standard, which is now also a Kenyan standard, KS ISO 22301:2012. In 2010, KEBS implemented an Information Security System in line with the ISO 27001:2005 standard in four departments: ICT, Human Resources, Metrology and Certification Body. This standard was aimed at the preservation of Confidentiality, Integrity, and Availability (C.I.A.) of information that guarantees business continuity and minimizes business loss by detecting and preventing security incidences. According to (Whitehorn, 2010), BCMS cannot be effective without reference to Information Security Systems. KEBS undertook the initiative of implementing BCMS within the organization as a first step. This was preceded by training on BCMS, which took place in October 2013. The objective of this training was to create awareness on the requirements of BCMS to trainees (KEBS) and to develop capacity for internal audits within KEBS. The KEBS National Quality Institute has been offering trainings on risk management in accordance with ISO 31000:2009 and is therefore equipped with the expertise in this field.

KEBS' implementation of BCMS depends on the implementation of BCMS requirements, which include the context of an organization, leadership commitment, planning, support, operational requirements, performance evaluation and improvement. The focus of this study was on leadership commitment, context of organization and operational requirements.

At the apex of KEBS' governance structure is the Board, National Standards Council (NSC). The Managing Director (MD) is responsible for the day-to-day administration of KEBS within the broad policy guidelines formulated by the NSC. For BCMS to flourish, top management commitment is mandatory. Business managers are described by (Hiles, 2007) as the custodians of business interests and responsibilities. The top management is responsible for defining the business continuity policy in terms of the organization's objectives and obligations. Their role in performance of BCMS cannot be underestimated.

KEBS has 856 employees out of which 550 employees are at the Headquarters in Nairobi (as of August 2014). KEBS activities include standards development, testing and calibration, quality assurance, inspection and certification, training, as well as support activities like human resources, procurement and marketing. As a government body, KEBS is supported by the Government of Kenya. It provides services to Kenya's citizens and industry in terms of standardization. Its context is therefore key in the implementation of BCMS. As a government body, KEBS experiences political influences in its operations and this aspect cannot be ignored. The implementation of BCMS requirements will enable KEBS to evaluate among others, the social, cultural, technological, natural and competitive environment. The requirements of BCMS consider key drivers and trends having an impact on the objectives and operations of KEBS. KEBS already faces competition in management system certification by Bureau VERITAS, BSI and others, and new trends are emerging, e.g., outsourcing of laboratory services and accreditation of laboratories by Kenya National Accreditation Services (KENAS). All these challenges require an operations strategy that is reflected in the BCMS implementation.

Operational requirements include business impact analysis (BIA), risk assessment (RA), BC strategy, BC procedures, as well as exercise and testing of the BC procedures. In assessing risks and BIA, KEBS requires the knowledge of its strategic

position in the economy, its brand/image, its key suppliers and customers, its products and how vulnerable it is to socio-political changes. A Business Continuity strategy is needed to protect, stabilize, continue, resume and recover its prioritized activities by mitigating, responding to and managing impacts to BC (ISO 22301). Procedures need to be put in place to guide and ensure continuity.

1.2 Problem statement

Disaster recovery, BCP and BCM are key to continued operation of any organisation (Shivo, 2010). In today's global economy, virtually every aspect of a company's operation is vulnerable to disruption, and the risk and cost of disruption extend well beyond information technology (IT) (Ernest&Young, 2012). As Charles Darwin quoted, "it is not the strongest or most intelligent that survives, it is the most adaptable to change" (Whitehorn, 2010). According to the Victorian Managed Insurance Authority (VMIA, 2012), a BCM program enables organizations to minimize legal liabilities, protect or enhance reputation, help achieve organization's objectives and goals and contributes to organizational resilience. The gap which this study fills is to investigate the awareness of Kenyan organizations of the existence of, as well as the need for and importance of having a BCMS, using KEBS as example. KEBS needs to practice what it preaches to earn the nation's confidence. Within the East African Community (EAC) member states, Kenya is leading in terms of standardization, which is why KEBS took the initiative to adopt the ISO BCMS standard. The absence of certification to the BCMS standard in Kenya exposes organizations of all kinds to disruptions, which they likely will not be able to handle properly in the absence of a holistic business continuity management system.

In Kenya, according to the Ministry of State for Special Programmes (2013), a high frequency of disasters hasresulted in a focus ondisaster-response, and leaving little time for risk-reduction initiatives. A shift in the mindset from response to risk management has yet to be fully realized, even within the political cycles. This has resulted in a low prioritization of risk reduction initiativeswhen it comes to allocation of national budgets. This should be resolved once the expected policy on risk management comes into effect, guiding allocation of funds towards risk reduction.

From the 2012 statistics of the United Nations International Strategy for Disaster Reduction, (UNISDR, 2014) covering 2000 to 2012, the economic and human impact of disasters was: $1.7 trillion dollars were lost, 2.9 billion people affected and 1.2

million people were killed. The government of Kenya has developed a National Policy on disaster management and disaster response through the Ministry of State for Special Programs (MOSSP). No regulation is in place on business continuity management system in Kenya and yet, organizations do not just face disasters of the nature addressed under the disaster management policy. The amount of critical information held by parastatals is very important for efficiency and effectiveness in service delivery (Mathenge, 2011). Aside from natural disasters, e.g. floods, and terrorist attacks, a devastating fire in KEBS laboratories, for example, would mean that KEBS could not test products until a new building is identified or new equipment has been bought. Will KEBS outsource the testing activities, and will its image be restored afterwards? How prepared is KEBS to return to business after an unforeseen incident? Are the systems currently in place able to address sudden changes in KEBS operations? This study unveils the level of awareness at KEBS of its identified risks and uncertainties.

ISO 22301:2012 is an international standard on business continuity management. International standards are considered to be the main driver for many aspects of BCM practice (Ihab, Sawalha, & Anchor, 2012). Further studies on BCP in class B and C parastatals in Kenya were recommended by (Mathenge, 2011), but KEBS was not part of the past study. No further studies have therefore been conducted on BCMS at KEBS.

This study evaluates the preparedness of KEBS to resume full business operations in case of a disruption and the level of awareness of KEBS' employees in terms of implementation of an inclusive, holistic BCMS.

There are very few empirical studies on the use and practice of BCM and the focus has mainly been on Europe and the USA (Ihab, Sawalha, & Anchor, 2012). This study therefore focuses on Kenya. The relationship between BCM and risk management is partly covered in this study as far as risk assessment is concerned. This relationship is supported by (ST-Germain, Aliu, Lachapele, & Dewez, 2012), citing that implementation and execution of risk assessment as a requirement under operations management in BCMS needs reference to risk management. BCMS is a more holistic and enterprise-wide system than BCM.

1.3 Research questions

The study was guided by the following research questions:

a) What systems are in place to address KEBS' business continuity?

b) How committed is leadership and top management in implementation of BCMS at KEBS and how have BCMS operational requirements been implemented at KEBS?

c) What is the level of awareness of the major threats to BC at KEBS?

d) What hurdles does KEBS encounter in the implementation of BCMS?

1.4 General Objective

The overall objective of the study was to evaluate the implementation of a Business Continuity Management System (BCMS) at the Kenya Bureau of Standards (KEBS).

1.4.1 Specific objectives

The study was guided by the following specific objectives.

The study intended:

a. To identify systems put in place to address business continuity at KEBS.
b. To determine leadership and top management commitment in the implementation of the BCMS and establish the implementation of BCMS operational requirements at KEBS.
c. To determine the level of awareness of the major threats to BC at KEBS.
d. To identify the hurdles in the implementation of BCMS at KEBS.

1.5 Value of the study

This study is important in several ways, especially to KEBS in evaluating the extent of its BCMS implementation. With the results of this study, KEBS is better placed to knowing what is missing on the road towards full implementation of BCM. The aim of this BCM implementation is to prepare KEBS to handle any form of disruption, stay in business after a disruption and also to help develop resilience to such disruptions. This study allows KEBS to evaluate the level of awareness towards BCMS within the organization, assess the greatest risks it is exposed to and respond to challenges in its BCMS implementation.

The study enlightens the government of Kenya on the need to have a business continuity management system in government bodies that is holistic in nature. The government spends billions of Kenyan shillings in many parastatals, including KEBS,

since their existence and operational continuity is of paramount importance to the government. According to (Zawada & J, 2003), regulations and guidelines are an excellent approach to ensure compliance with best practices. The government of Kenya, from this study, is able to recognize the need for implementing BCMS as a must-have requirement in government organizations, just like it did with ISO 9001. By comparison, the adoption of BCM in certain parts of the UK economy is actively promoted by Government policy there (Pearson & Woodman, 2012).

The study is of importance to other researchers in this field of study by contributing to the existing body of knowledge in operations management strategy. The study will be used as a reference and in identifying areas for further research.

Insurers would benefit from creating products that reflect BCM. Insurers should do more to promote the implementation of BCM to their clients (Pearson & Woodman, 2012). Their influence could be critical in improving the widespread adoption of BCM, yet currently insurers are low on the list of drivers of BCM, despite the premium structure of some insurance companies.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

The challenge of recovering from disruptions goes beyond providing an emergency response plan or using disaster management strategies that were previously used (ST-Germain, Aliu, Lachapele, & Dewez, 2012). Organizations of all sizes and types should now engage in a comprehensive and systematic process of prevention, protection, preparedness, mitigation, and response for business continuity and recovery. It is no longer enough to draft a response plan that anticipates and minimizes the consequences of naturally, accidentally, or intentionally caused disruptions. Rather, organizations must also take adaptive and proactive measures to reduce the likelihood of a disruption. ISO 22313:2012, an international standard on guidelines for business continuity management systems, states that business activities are disrupted by a wide variety of incidents, many of which are difficult to predict or analyse. By focusing on the impact of disruption rather than the cause, business continuity identifies those activities on which the organization depends for its survival, and enables the organization to determine what is required to continue to meet its obligations.

Today's threats require the creation of an on-going, managed process that ensures the survival and sustainability of an organization's core activities before, during, and after a disruptive event. The ability of an organization to recover from a disaster is directly related to the degree of business continuity planning that has taken place before the disaster. According to (Mathenge, 2011),"the continued management of operations depends to a large extent on management's awareness of potential disasters, their ability to develop plans to minimize disruptions to critical functions and the ability to conduct recovery operations successfully with the least amount of downtime."

2.2 Business Continuity Management System

According to (Ihab, Sawalha, & Anchor, 2012) BCM has its roots in IT disaster recovery planning, which was first implemented in the late 1970s. The main focus during the 1970s and 1980s was to ensure the continuity and quick recovery of mainframe computing systems, whereas less attention was given to business and work area continuity and recovery. There has been a shift in the scope of BCM from an IT-

based process into an enterprise-wide and strategic activity that encompasses all business areas.

The discipline has evolved as a management process for identifying potential system failures and for preparing contingency plans to enable the organization to continue key operations whilst a total system rebuild is undertaken, in the aftermath of disaster or other business interruption (Ethné Swartz, 2003).

According to (Pearson & Woodman, 2012), two new International Standards in business continuity (ISO 22301 and ISO 22313) will further increase the use of international best practice in business continuity. ISO 22301 is an ISO standard that specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to prepare for, respond to and recover from disruptive events when they arise. ISO 22313 is a guideline standard to BCMS.

According to ISO 22301, Business Continuity Management is a holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

The failure of a business continuity plan, which is part and parcel of BCMS, has many effects but the major one is the much longer time requirement to get back to business after an outage. The time it takes to resume business activities is one issue, but the cost to do so can be exorbitant in some cases (Hotchkiss, 2010). BCMS encompasses and includes BCP, and is based on processes and their interactions. Planning is only a segment of management; it is the one mostly dealing with decision-making, allocation of resources and time, and sequencing of activities (ILO, 2011). VMIA states that a "BCM program enables organizations to minimize legal liabilities, protect or enhance reputation, help achieve organization's objectives and goals and contributes to organizational resilience" (VMIA, 2012).

Through business, an organization can recognize what needs to be done to protect its resources (e.g. personnel, premises, technology and information), supply chain,

interested parties and reputation, before a disruptive incident occurs. With that recognition, the organization is able to take a realistic view on the responses that are likely to be needed as and when a disruption occurs, so that it can be confident of managing the consequences and avoiding unacceptable impacts. It is a broad process that includes data collection and analysis for decision making, implementation of the plan of action and evaluation of the whole process for learning purposes. "Today, good business continuity management is not about being forced into taking action to address external pressures. It is about recognizing the positive value of Business Continuity good practice being embedded throughout your organization" (ST-Germain, Aliu, Lachapele, & Dewez, 2012).

2.3 Importance of BCMS

According to the British Standards Institute (BSI) 2012 training manual, BCMS is important in the identification of threats and the impact of these threats to the operations of an organisation. It is further important in the provision of a framework for building organizational resilience, provision of effective responses and in safeguarding the interests of key stakeholders, the organization's reputation, as well as its brand and value creating activities. An effective business continuity management process will address compliance issues, provide for maintenance and protection of vital records, address health and safety issues, improve overall security and help avoid liability actions (ST-Germain, Aliu, Lachapele, & Dewez, 2012).

Three main drivers for the broad awareness of the importance of BCM, according to (RSA-ARCHER, 2012), include 24/7 service delivery requirements, globalization and an ever expanding and increasingly complex supply chains and increasing operations risks due to frequent disruptive events.

The BCMS standards (ISO 22301 and ISO 22313) not only improve the understanding of and resilience against business risks, but they help to meet an organization's customers' needs and can give an organization a significant competitive advantage (Pearson & Woodman, 2012). By assuring continuity, BCMS instills confidence in employees, customers and suppliers. Everyone is then able to give their best performance with the knowledge of continuity after disaster strikes. Business continuity can be effective in mitigating impacts in different situations. This can be conceptually illustrated, as shown in Figures 2.1 and 2.2 below.

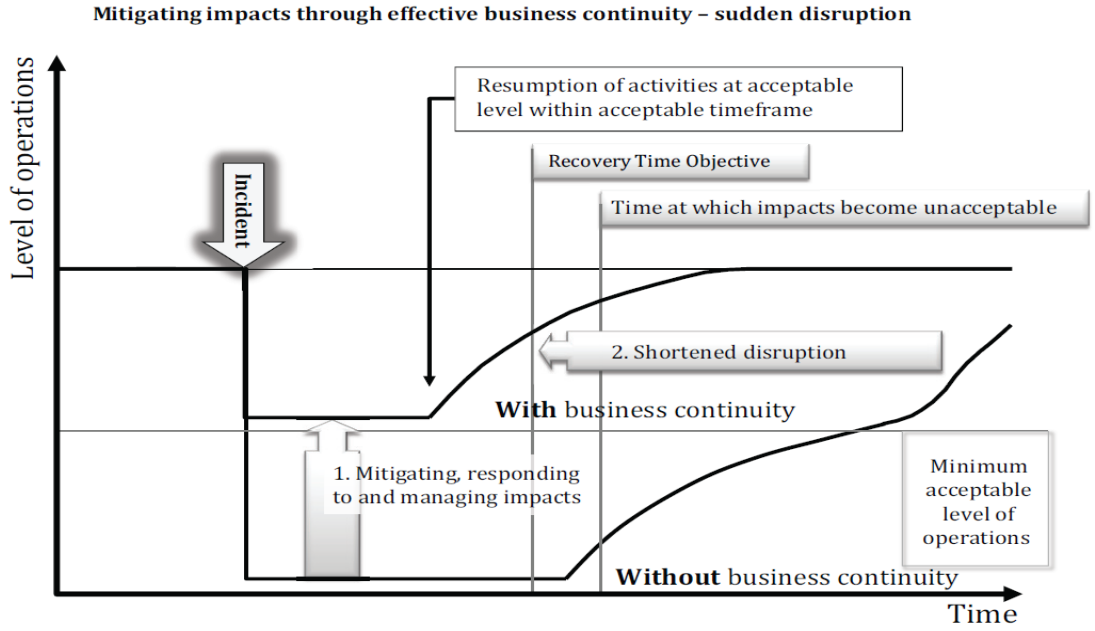

Figure 2.1.Illustration for business continuity being effective for sudden disruption

(Source: ISO 22313:2012)

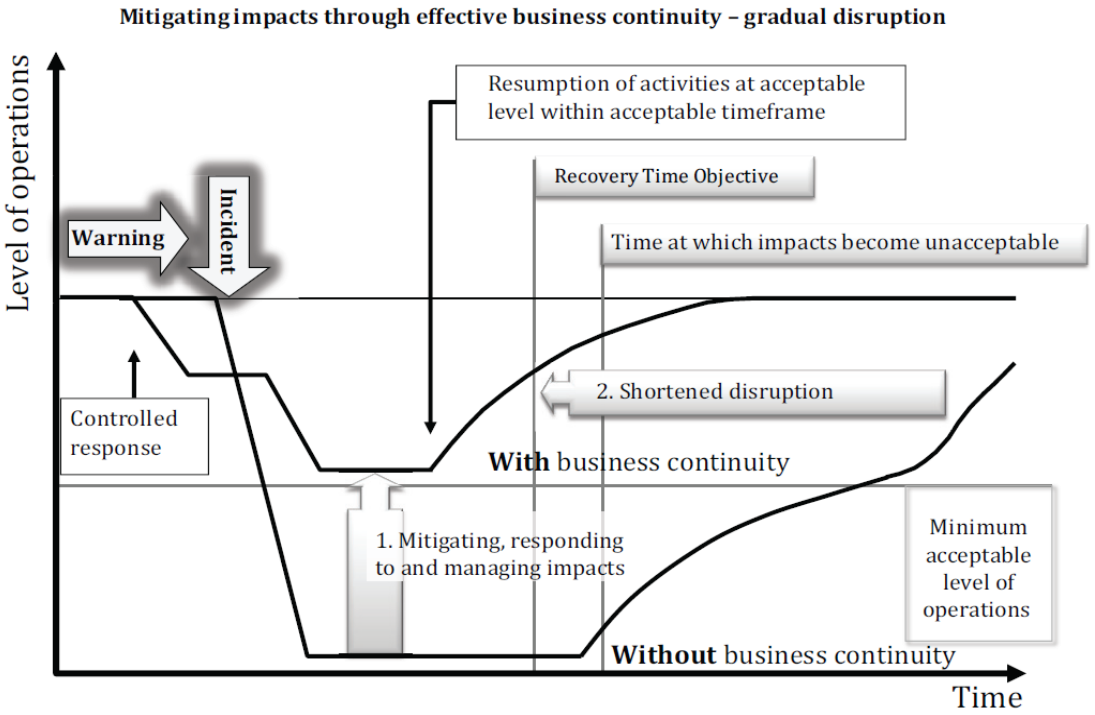

Figure 2.2.Illustration for business continuity being effective for gradual disruption (e.g. approaching pandemic)

(Source: ISO 22313:2012)

The two diagrams illustrate how operations will not go below minimum acceptable levels in situations with applied business continuity measures, regardless whether faced with sudden or gradual disruptions. In both cases, recovery time to full operational performance is also shorter than in systems without business continuity measures.

2.4 Examples of Disruptions

The destruction of the World Trade Center (WTC) in New York City in 2001 also highlighted the need for business continuity management (BCM). Despite the loss of staff, offices, files and computer hardware, Morgan Stanley was able to announce within days that they were ready to resume full operations and reassured their clients that their assets were safe and their financial advisors were hard at work contacting their individual investors to answer questions and address their concerns (Ethné Swartz, 2003).

In a white paper released by CDP (CDP, 2014), heavy spring and summer rains led to American Electric Power Company's inability to deliver coal to a power plant in Indiana. For the first time in its history, the Cook Coal Terminal in Metropolis, IL, which receives Powder River Basin Coal by train and loads it onto barges was unable to deliver coal because the Ohio River water level was too high. Johnson Control (2011) reported that their New Orleans operations and associated personnel had been severely impacted by hurricane Katrina, which resulted in the eventual relocation of the operations to higher ground in Louisiana and Texas. The move disrupted a highly profitable operation and ultimately cost the company hundreds of thousands of dollars in lost revenue and costs associated with helping their employees relocate.

When news of the massive 9.0-magnitude earthquake and subsequent tsunami, which struck Japan in 2004, reached the business continuity management team of Systems on Silicon Manufacturing Company Pte Ltd (SSMC), the team immediately responded by holding an emergency meeting and triggering its Business Continuity Plan (BCP) on the very evening of the disaster. Due to this quick action upon an

existing BCP, SSMC emerged unscathed, enjoying a continued supply of materials, spares and tools resulting in no business loss. This success can be attributed to SSMC's ferventness in Business Continuity Management (BCM) (Systems on Silicon Manufacturing Company Pte Ltd, 2014).

On the other hand, Ace Limited recorded net pre-tax catastrophe losses in 2011 of $859 million, which included weather related events in the USA (Superstorm Sandy), Australia and Thailand (flooding) (CDP, 2014).

2.5 BCMS Requirements

A BCMS, like any other management system, has five key components (ISO 22301:2012) which include a policy; people with defined responsibilities; management processes relating to policy, planning, implementation and operation, performance assessment, management review, and improvement; documentation providing auditable evidence; and specifically, any business continuity management processes relevant to the organization.

Business continuity measures also contribute to a more resilient society. The wider community and the impact of an organization's environment on the organization itself and other organizations may need to be considered in the recovery process (ISO 22301). BCMS is an operations management strategy. In operations management, an input that goes through processes/transformations gives rise to outputs. In this case, BCMS takes interested parties' requirements as inputs for BCM and through required actions and processes, produce business continuity outcomes (i.e. managed business continuity) that meet their requirements. This mechanism is illustrated in Figure 2.3 below, in terms of a Plan-Do-Check-Act (PDCA) model.

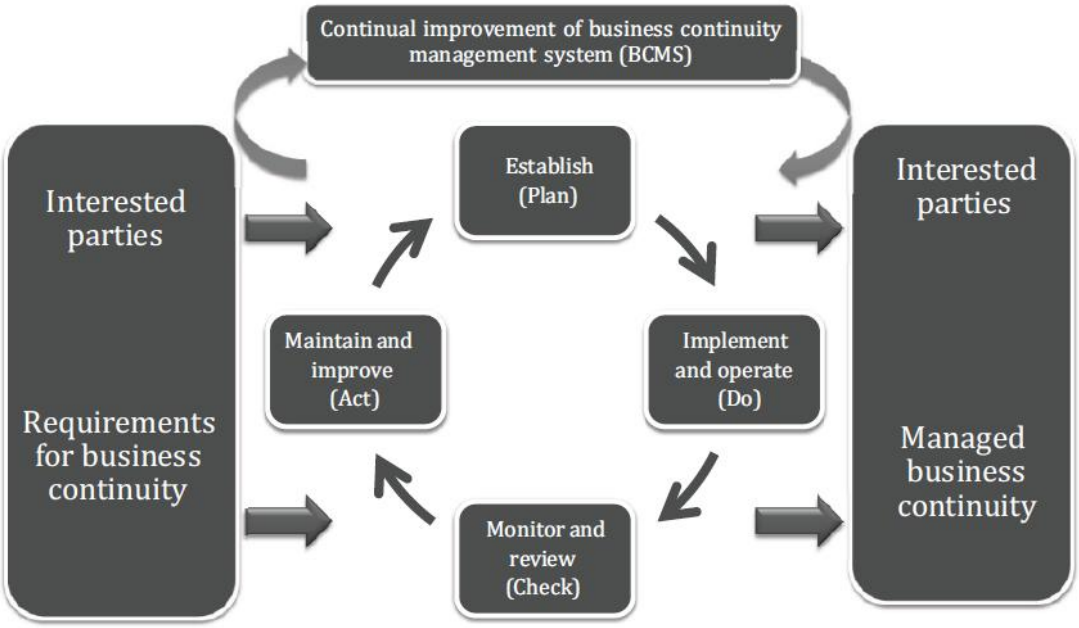

Figure 2.3 PDCA model applied to BCMS processes.

(Source: ISO 22313:2012)

The performance of a BCMS relies on the implementation of its requirements, which include context of an organization, leadership commitment, planning, support, operational requirements, performance evaluation and improvement.

2.5.1 The organizational context and BCMS

An organization needs to determine external and internal issues related to the purpose of the organization's existence, both of which will affect the outcome of the implementation of its BCMS. Such issues include the organization's activities, functions, services, products, partnerships, supply chains, relationships with interested parties, and the potential impact related to a disruptive incident. They further include links between the business continuity policy and the organization's objectives and other policies, including its overall risk management strategy, as well as the organization's risk appetite. All these issues are expected to be identified and documented. According to (Hiles, 2007), an organization's risk appetite is a definition of each level of risk which it is prepared or able to accept and this should be reviewed regularly to keep pace with the organisation's changing business objectives and risk tolerance. The needs and expectations of interested parties relevant to BCMS include legal and regulatory requirements. The scope includes the extent of the application of

the BCMS. This scope is important and should be defined in terms appropriate to the size, complexity, and nature of the organization. The scope is the part of the requirements that guides the organisation on documenting the goals, mission, legal and regulatory responsibilities, obligation to internal and external stakeholders, and its products/service and related activities. It actually defines the organisation as a whole. It is also necessary to state exclusions in the application of BCMS. These exclusions, according to ISO 22301, shall not affect the organization's ability and responsibility to provide continuity of business and operations that meet the BCMS requirements, as determined by business impact analysis or risk assessment and applicable legal or regulatory requirements. An organisation shall be required to establish, implement, maintain and continually improve a BCMS (ISO 22301:2012).

2.5.2 Leadership and BCMS

For any management system to be applied in an organization, top management commitment is mandatory. Their commitment and leadership in implementing the BC policy and objective is of utmost importance. Business managers are described by (Hiles, 2007) as the custodians of business interests and responsibilities. They must practice good stewardship. The management cannot be said to be fulfilling this duty if an unplanned event can jeopardize the survival of the organisation. "Through its leadership and actions, management can create an environment in which different actors are fully involved and in which the management system can operate effectively in synergy with the objectives of the organization"(ST-Germain, Aliu, Lachapele, & Dewez, 2012). "Responsibility of BCM sits with senior management" (Woodman & Hutchings, 2010).

ISO 22313 states that top management should provide evidence of its commitment to the development and implementation of BCMS and to continually improving its effectiveness. The top management is responsible for defining the business continuity policy in terms of the organization's objectives and obligations. The policy needs to be well communicated throughout the organisation and made available to interested parties and needs to be complimentary to other relevant policies. The top management should also communicate and assign responsibilities and authorities. Executive sponsorship is a key input to the success of the business continuity. According to (Ian, 2009), successful business continuity management requires a commitment from the

executive to raising awareness and implementing sound approaches to build resilience.

2.5.3 Operational Requirements

Business Impact Analysis (BIA), one of the operational requirements for BCMS, enables an organization to identify the critical processes that support its key products and services, as well as the interdependencies between processes and the resources required to operate these processes at a minimally-acceptable level (ST-Germain, Aliu, Lachapele, & Dewez, 2012). BIA is invaluable in justifying spending on protection and recovery capabilities (Shivo, 2010). The BIA enables the organization to prioritize for resumption of those activities that support its products and services. The purpose of a business impact analysis according to ISO 22313:2012 is to obtain an understanding of the organization's key products and services and the activities that deliver them; determine priorities and timeframes for resuming activities; identify the key resources likely to be required for continuity and recovery; and identify dependencies (both internal and external).

Risk assessment is another operational requirement and promotes understanding of the risks to prioritized activities and their dependencies and the potential consequences of a disruptive incident. It studies all aspects of threats including physical, administrative, environmental and technical measures (Shivo, 2010). Risk assessment provides a structured process for analysing risk in terms of consequences and likelihood before deciding on further treatment that may be required. It involves risk identification, consequences in case the risk happens, the likelihood of the risk happening and anything that might mitigate the consequences or reduce the likelihood of the risk occurring (ISO 22313:2012).
Risk management is the cornerstone of BCM effectiveness (Ihab, Sawalha, & Anchor, 2012).

A Business Continuity Plan (BCP), a third operational requirement, should provide a framework that builds organisational capability to respond to threats and safeguards the interests of key stakeholders, reputation, brand and value-adding activities. It may contain numerous elements, the most common being "strategies for maintaining and/or recovering all activities which enable key products and services" (Pearson & Woodman, 2012).

Business Continuity Strategy is another operational requirement and involves the identification and evaluation of a range of business continuity strategy options and enables the organization to choose appropriate ways of preventing disruption of its prioritized activities and dealing with any disruptions that take place. Determining the business continuity strategy involves identifying the actions required to address the findings from the BIA and risk assessment and implementing them in such a way that the business continuity objectives of the organization are met. Such actions are likely to be needed before, during and after a disruptive incident (ISO 22313). The resulting business continuity strategy will provide for the resumption of activities at an acceptable level of operation and within agreed timeframes. Early provision of an overall organizational BCM strategy will ensure that BCM activities are aligned with and support the organization's overall business strategy. The BCM strategy should be an integral component of an institution's corporate strategy (ST-Germain, Aliu, Lachapele, & Dewez, 2012). A cost benefit analysis compares the benefits and costs incurred for a certain measure (Ian, 2009). Typically, the lower the maximum tolerable period of disruption, the more costly and complex the recovery treatment is going to be. The chosen strategies need to take into account any risk treatment that is already in place within the organization. BC Strategy involves the protection, stabilizing, continuing, resuming and recovering of activities already prioritised by the organisation as key to its continuity. Business continuity strategy, according to ISO 22313, includes relocating business activities, resource relocation or reallocation, creating or having alternate processes or spare capacity, resource and skills replacement and workarounds including manual work instead of automated processes. Many organisations have mitigation measures for impact and duration and these include insurance, asset restoration and reputation management. Insurance, however, does not buy back the lost business, it only provides money and in some cases, the money comes later rather than sooner, with adverse implications for the organization's cashflow (Hiles, 2007). Other strategies include evaluating the BC of suppliers through supplier audits. Implementing resource requirements in the BC strategy is a good consideration. This should include personnel, information and data, building, work environment and associated utilities, inventory supplies of prioritised activities, ICT, transportation, suppliers, and finance. Determining ways of reducing the likelihood of risk occurrence, shortening the period of disruption and limiting the impacts of disruption are generally important.

The fifth operational requirement is Business continuity procedures which establish appropriate internal and external communications protocols, are specific, flexible, and focussed on impacts of events and are effective (ST-Germain, Aliu, Lachapele, & Dewez, 2012). One of these procedures is the Incident Response procedure and its management structure, which are created as a result of BCMS implementation and enable an organization to prepare for, mitigate, and respond effectively to disruptive incidents (ISO 22301). The Incident Response structure should be simple and capable of being executed quickly. Another procedure is for warning and communication which include procedures for the detection and regular monitoring of incidents and communications. This procedure should be regularly exercised.

Documented procedures that enable organizations to respond to an incident and deal appropriately with the resumption and recovery of its activities are important (ISO 22313). Hiles (2007) describes a business continuity plan as a business management plan rather than a technical plan. Business continuity planning is a systematic approach whose objectives are to improve the organisation's resilience and to manage incidents in the event of a disruption (Shivo, 2010). It is through a careful assessment of a company's operation that a viable business continuity plan is developed (Metzler, 2014). Sensitivity to the loss of current data and the ability of personnel to operate from various locations are considerations for ease of implementation of business continuity solutions. A procedure for responding to a disruptive incident and how the organization will continue or recover its activities within a predetermined timeframe is therefore key and needs to be described in the business continuity plan.

A fourth procedure is aimed for recovery and is used in restoring and returning business activities to normal after an incident (ISO 22301:2012). According to (NSW, 2005), a Management Recovery plan declares a disaster, invokes business unit recovery plans and monitors recovery at the highest level. A business unit recovery plan recovers essential business operations belonging to individual business units. Testing of BC procedures ensures that organisations are consistent with BC objectives. Organisations therefore need to have frequently scheduled tests in their test plans, where independent observers validate the tests and their results (Mathenge, 2011). "Continuity testing examines the comprehensiveness and applicability of the developed plans and their ability to cope with various disasters and crises" (Ihab,

Sawalha, & Anchor, 2012). Exercises and the documented results of exercises are used to ensure the effectiveness and readiness of business continuity plans. Testing raises awareness and creates confidence that the approach and strategies adopted could be used in the event of a genuine incident. Good BCM practice involves regularly exercising or rehearsing the BCP (Pearson & Woodman, 2012). This enables plans to be revised, refined and updated before weaknesses are exposed by a real disruption. "Exercising and testing are the processes of validating business continuity plans and procedures to ensure the selected strategies are capable of providing response and recovery results within the timeframes agreed to by management" (ST-Germain, Aliu, Lachapele, & Dewez, 2012).

2.6 Conceptual Framework

This study examines the implementation of the Business Continuity Management System at the Kenya Bureau of Standards. In this case, the Business Continuity Management System requirements are the independent variable while its performance at KEBS is the dependent variable. The implementation of the three requirements together will lead to more awareness of BCMS within and outside of KEBS (stakeholder awareness). KEBS, in turn, will be in a position to identify its key vulnerabilities through knowing its risk appetite and threats to BC, and by having a risk management in place and performing a business impact analysis, among other operational requirements. KEBS will be in a better position to adapt to new challenges to BC since BCMS is an operational strategy. The conceptual framework is illustrated in Figure 2.4.

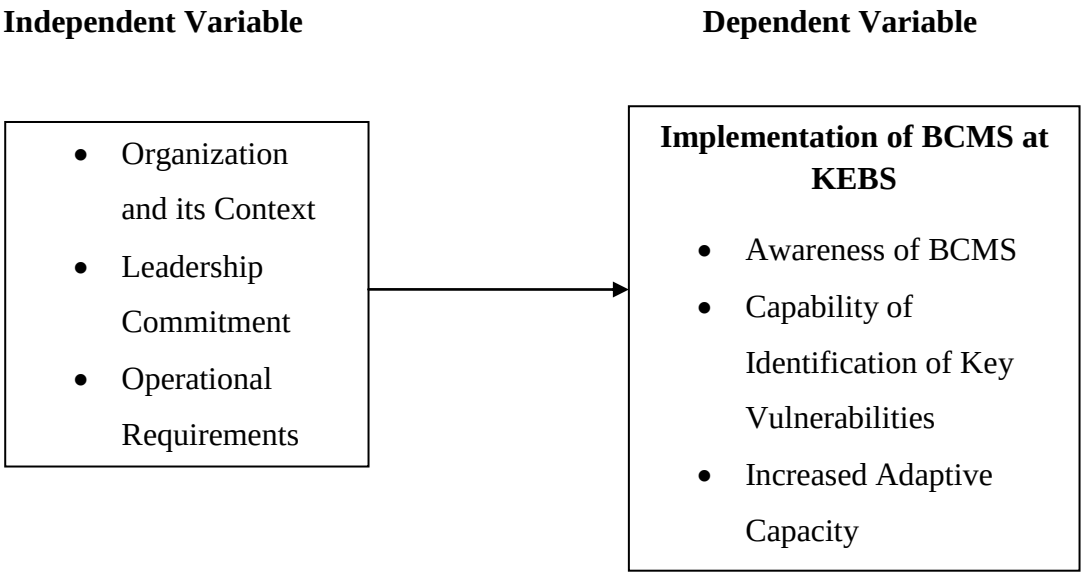

Figure 2.4 Conceptual framework

{Adapted from (Whitehorn, 2010)}

2.7 Summary

A lot of studies on BCM show that it has become a key operational strategy bearing in mind the uncertainty of disasters occurring and the economic loss associated with disasters. Business Continuity Management System, being generic, is applicable to all types, natures and sizes of organizations. A continent-by-continent survey carried out by the Business Continuity Institute, (Business Continuity Institute in association with BSI, 2014) revealed that overall, 44% of their respondents currently use ISO 22301 as a framework for their business continuity program and that in sub-Saharan Africa, around 65% of respondents were more likely to use ISO as a framework for BCM. BCMS standards ISO 22301 and ISO 22313 not only improve understanding of and resilience against business risks, but help to meet an organization's customers' needs and can give an organization a competitive advantage (Pearson & Woodman, 2012).

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter provides discussion on the research methodology, which was used in this study. It discusses the research design, sample size and sampling techniques, data collection methods, data analysis and data presentation methods and why they were the most preferred.

3.2 Research Design

This is a case study which allows gathering of in-depth information about the application of the Business Continuity Management System in KEBS.

The research design adopted is descriptive in nature. This approach was chosen because it enabled the researcher to collect in-depth information about the population being studied. A qualitative analysis approach was employed. Other researchers who have employed this design include (Mathenge, 2011).

3.3 Population

The population of this study consisted of four groups, including top management, operations managers, as well as technical and non-technical staff at KEBS. The study focused on top management because they are the policy makers, operations managers because they are the 'owners' of each function, and other staff because BCMS must be known, communicated, tested, exercised and implemented throughout the organisation. As of August 2014, KEBS had a total of 856 employees in all of Kenya's regions, while 550 out of the 856 were based at the headquarters in Nairobi. The study focused on the headquarters staff because BCMS, like all other management systems, can easily be implemented at the headquarters first and then propagated to regional offices.

3.4 Sampling

A stratified complex random sampling was used in this study because the sample did not constitute a homogeneous group. Kothari & Garg, (2014) describe stratified sampling as consisting of a population divided into sub-populations, which are individually more homogeneous. The population was divided into the top management group (CEO and directors of functions), operational management (heading departments), technical staff (officers) and non-technical staff. Simple random sampling was then used in each group (stratum). Since each stratum was

different from the others in terms of size and variability, disproportionate sampling design was used. Out of the 550 staff members at the KEBS headquarters, 60 employees were selected for the study, representing the four strata. Good accuracy levels can be achieved at relatively small sample sizes, provided that the samples are representative, according to (FAO, 2014). This number was satisfactory for the case study since a higher number could not have brought much difference in the findings because all employees were represented in each stratum. BCMS being a system, knowledge within each stratum was assumed to be the same because each stratum was homogeneous. According to (Kothari & Garg, 2014), the sample size under each stratum is found by using Formula 1, and the sample sizes for this study are summarized in Table 3.1.

$$n_i = nP_i \quad \textbf{(1)}$$

Where: n = total sample size,

n_i = number of elements selected from stratum *i*

P_i = proportion of population included in stratum *i*

For example: Sample size from the 274 non-technical staff members:

n_i = 60 x 274/550 = 29.9 = 30 persons.

Table 3.1 Stratified random sampling frame

Cadre at Headquarters (stratum)	Managing Director and Directors	Heads of Departments	Officers	Non-technical Staff	Total
Total number of staff at headquarters	7	20	250	274	550
Sample size	1	2	27	30	60

3.5 Data Collection

Primary data was obtained through self-administered questionnaires. The study included 60 key informants, divided in four strata as detailed above. The study tool (questionnaire) was piloted and standardized using 10 respondents and found to be

suitable for the study. These 10 pilot structured questionnaires were interviewer administered to motivate respondents to complete the entire questionnaire and provide relevant data, according to (Ihab Hanna, 2012). Then, the remaining 50 structured questionnaires with binary and Likert scale questions were administered to the staff according to their cadre. These questionnaires were self-administered because it was concluded that the respondents were comfortable with the instrument and questions therein.

The questionnaire was divided into 6 focal sections: section A was about the Respondent Profile. The respondent profile was important to ensure the proportional distribution among the four strata (cadre) and since the performance of one group (top management commitment) was being evaluated, the profile ensured the group did not evaluate itself. Each stratum consisted of staff with differing roles and knowledge about BCMS and this awareness was one of the main objectives of the study. The need for how long respondents had worked at KEBS helped in knowing if the objectives were affected by work experience at KEBS. Section B was on the Context of the Organization; section C on Leadership and Top Management Commitment; section D on Operational Requirements; section E on Major Threats to the BC, and section F on Challenges in the Implementation of BCMS. The administered questionnaire can be found in Appendix 1.

3.6 Data Analysis

The data collected was quantitatively analyzed. The responses from individual respondents were compared and summarized according to the objectives of this study. Analysis was performed using Statistical Package for Social Scientists (IBM SPSS statistics version 20) and Microsoft Excel. Statistics from the analysis were presented in tables and graphs.

CHAPTER FOUR: DATA ANALYSIS, FINDINGS AND INTERPRETATION

4.1 Introduction

This chapter presents analysis and findings of the study. The study findings are presented on the business continuity management system at the Kenya Bureau of Standards. The data was collected exclusively through the questionnaire, which was designed to meet the objectives of this study.

4.1.1 Response Rate

The study targeted 60 respondents, 10 of which were used for piloting and standardization and these were not included in the analysis. The 50 structured questionnaires with binary and Likert scale questions were administered to the staff according to their cadre. The distribution of respondents is depicted in Figure 4.1. The questionnaire was filled in and returned by 50 out of 50 respondents, resulting in a response rate of 100%.

4.2 Data Analysis

4.2.1 Respondents' Profile

The study sought to find out the respondents' profile in terms of designation. The majority of the respondents were officers (46%), followed by non-technical staff (42%) and department heads (8%), while the smallest fraction was the directorate with 4% of respondents. The percentages gave an informed decision on awareness and also, objective response on top management commitment was received since they made the smallest percentage of respondents. The composition of the respondents is shown in Figure 4.1.

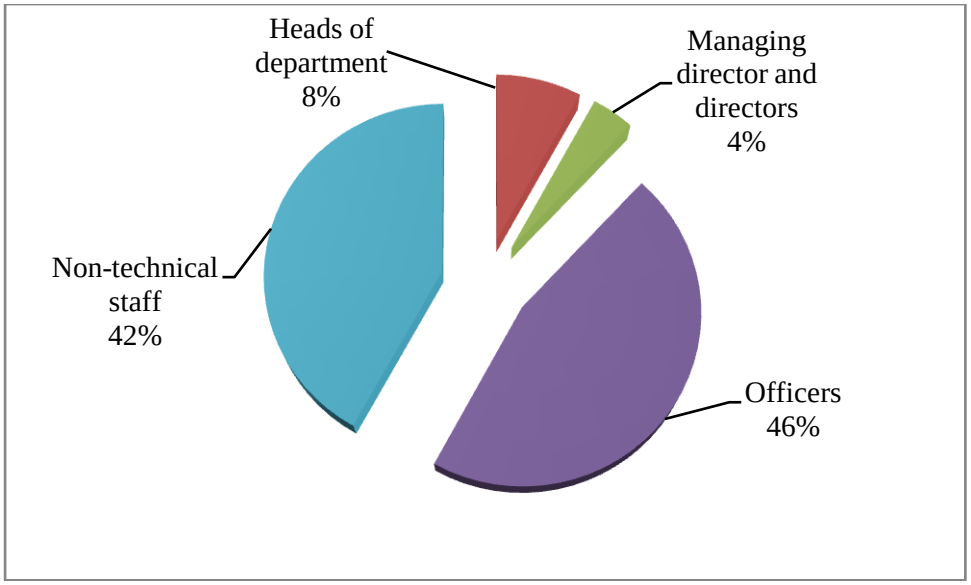

Figure 4.1 Respondents from various cadres

Evaluating how long the respondents had worked at KEBS, it was found that 54% (n=27), the majority of the respondents, had worked at KEBS for a duration of 1-10 years, while those who had worked for over 31 years formed the least proportion of 8% (n=4), while 10% (n=5) of the respondents did not declare for how long they had worked at KEBS. This means that the results of the study were based majorly on experience of staff members who had worked for KEBS for less than 31 years. This information is shown in Table 4.1 and Figure 4.2.

Table 4.1 Period the respondents had worked for KEBS

Duration in years	Percentage and number of respondents
1-10 years	54% (n=27)
11-20 years	18% (n=9)
21-30 years	10% (n=5)
31 years and above	8% (n=4)
Not indicated	10% (n=5)

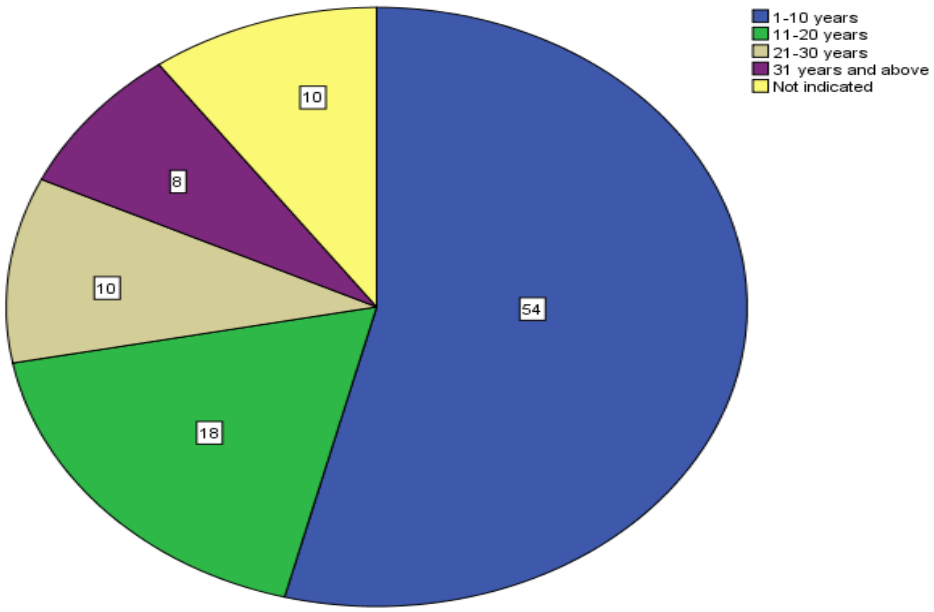

Figure 4.2 Period of time (in years) the respondents had worked for KEBS

4.2.2 Systems in Place to Address BC

To identify the knowledge about systems put in place addressing business continuity at KEBS, the respondents were asked to tick either "yes" or "no" on whether they were aware of various systems relevant for the context of the organization, as far as BCMS is concerned, had been established at KEBS. It was found that the majority of respondents (68%, n=24) were in agreement that systems are in place that identify and document KEBS' functions and products, as well as the impact of a disruptive incident on such functions and products. Almost one quarter of the respondents (24%, n=12) answered with "no" and 8% (n=4) did not indicate whether they knew of these systems being in place or not. The question on whether links between KEBS' objectives, policies and risk management strategy are identified and documented, a significantly high number of the respondents agreed (72%; n=36) that these links were identified and documented, while 26% (n=13) disagreed, and only one respondent did not indicate if they were aware of these links or not. The replies to these two questions clearly demonstrate that systems on context of organization are in place at KEBS but are either not fully functional or known by staff, and/or their existence has not been effectively communicated to all staff.

Regarding risk appetite, 44% of the respondents agreed that risk appetite had been identified and documented while a slightly higher proportion of 48% disagreed. However, 8% did not answer the question on the identification of risk appetite. Asked whether the uncertainty that gives rise to risk had been defined, 40% indicated that this had been defined, while 56% disagreed and 4% did not answer this question. Half of the respondents (50%) disagreed that risk criteria were set, taking into account the risk appetite, while 44% agreed, and 6% did not answer this question. These responses clearly demonstrate a lack of organization-wide awareness about the existence of systems on risk management at KEBS as far as risk appetite, the uncertainty that gives rise to risk, and risk criteria are concerned. Yet, these systems exist at KEBS.

Asked whether business continuity objectives had been articulated, 58% of the respondents indicated that these had been articulated, while 36% said “no” and 6% did not commit. The purpose of the BCMS at KEBS was defined according to only 40% of the respondents, while 54% were not aware of its definition and 6% did not respond to this. According to 50% of the respondents, interested parties relevant to the BCMS and their requirements were determined, while 48% did not believe so and 2% did not respond to this question. Equal proportions of the respondents believed that procedures to identify, access and assess applicable legal and regulatory requirements related to business continuity of operations were available (48%), while 48% did not believe so, and another 4% did not disclose their stand. As far as the establishment of the scope, mission and goals of the BCMS was concerned, 50% of the respondents believed these were established, 42% believed they were not, while 8% did not respond to this question. These responses also indicate a significant lack of awareness of the existence of these BC systems.

Responses to this section made it evident that the knowledge of the existence of BCMS components resides with only a limited number of staff members at KEBS, which is likely due to lack of effective communication. The responses to the above questions are summarized in Table 4.2.

Table 4.2 Respondents' answers to the context of organization

Business systems in place	YES	NO	No Answer
Functions, products and the impact of a disruptive incident are identified and documented	68% (n=34)	24% (n=12)	8% (n=4)
Links of objectives, policies and risk management strategy are identified and documented	72 % (n=36)	26% (n=13)	2% (n=1)
Risk appetite is identified and documented	44% (n=22)	48% (n=24)	8% (n=4)
Business continuity objectives are articulated	58% (n=29)	36% (n=18)	6% (n=3)
Uncertainty that gives rise to risk is defined	40% (n=20)	56% (n=28)	4% (n=2)
Risk criteria taking into account the risk appetite are set	44% (n=22)	50% (n=25)	6% (n=3)
Purpose of the BCMS is defined	40% (n=20)	54% (n=27)	6% (n=3)
Interested parties relevant to the BCMS and their requirements are determined	50% (n=25)	48% (n=24)	2% (n=1)
Procedures to identify, access and assess applicable legal and regulatory requirements related to continuity of operations are available	48% (n=24)	48% (n=24)	4% (n=2)
Scope, mission, goals of the BCMS were established	50% (n=25)	42% (n=21)	8% (n=4)

4.2.3 Leadership and Top Management Commitment

Questions posed in this section sought to find out the commitment of the leadership and top management in the implementation of the BCMS at KEBS. Respondents were asked to indicate their perceived extent to which the Leadership has established, or committed to, the following steps on a scale from 1 to 5, where 1 = no extent at all, 2 = small extent, 3 = moderate extent, 4 = large extent, and 5 = very large extent.

Asked whether strategic policies and objectives for the BCMS had been established at KEBS, it was found that 8% of the respondents did not agree at all with the fact that management had established these. This is compared to 22% who agreed to a small extent, 40% to a moderate extent and 24% to a large extent, and 6% agreed to a very

large extent. Generally, the respondents affirm that the KEBS leadership and top management are committed to the establishment of strategic policies and objectives for the BCMS.

Asked to evaluate the integration of BCMS requirements into business processes, 10% indicated no integration at all, 18% to a small extent, 38% to a moderate extent, 26% to a large extent, 6% to a very large extent and 2% of the respondent did not respond. These answers also indicate that the KEBS management is committed to the integration of BCMS requirements into the business processes.

Queried whether resources for the BCMS were allocated and available, 20% of the respondents indicated no resources were allocated or available at all, 32% agreed to a small extent, 32% to a moderate extent, 8% to a large, 4% to a very large extent and 4% did not answer. About two thirds of the respondents did not believe there were enough resources allocated and available for BCMS, while 20% expressed complete lack in commitment in the form of resources. This demonstrates a low commitment by the leadership in terms of resources.

The importance of an effective BCM and conformity to the BCMS requirements was believed to have been well communicated to the staff. Communications to a small, moderate, and large extent were reported by 36%, 24% and 20% of the respondents, respectively and 4% reported that communication of the importance of BCM and conformity to BCMS was to a very large extent. 16% believed there was no communication to this effect at all. These results attest that KEBS staff is aware of the importance of an effective BCM and conformity to BCMS. This is critical because any management system is implemented through an organization's staff members and their knowledge of its importance is key to a successful implementation.

Asked whether direction and support for the effectiveness of the BCMS are provided to relevant management roles, it was found that 8% indicated not at all, 36% to a small extent, 30% to a moderate extent, 16% to a large extent and 10% to a very large extent. This confirms commitment by KEBS' top management in this area as this direction and support for effectiveness of a system has to originate from leadership/top management.

Continual improvement is promoted to a very large extent according to 6% of respondents, while 14% indicated no promotion at all, 16% to a small extent, 34% to a moderate extent, 26% to a large extent, while 4% did not reply. This shows a big proportion of the respondents supporting the fact that KEBS' leadership and top management are committed to the organization by promoting continual improvement, compared to a paltry 14% who did not report any such promotion at all.

Asked whether the business continuity policy is available and has been communicated and reviewed, it was found that 26% said not at all, 34% to a small extent, 20% to a moderate extent, 18% to a large extent and 2% did not indicate any extent. The big proportion of 72% of all the respondents support the notion, though to a varied extent, that the business continuity policy is in place and has been communicated to, and reviewed with, staff at KEBS. This question attracted the highest percentage of staff disagreeing that business continuity policy was available and communicated, at 26%, which is indicative of a low level of awareness and communication.

On the question whether BCMS plans and objectives had been established, it was found that 14% said not at all, 26% to a small extent, 34% to a moderate extent, 18% to a large extent and 8% to a very large extent. This makes a total of 86% of respondents supporting, though to a varied extent, the fact that BCMS plans and objectives have been established at KEBS.

Asked whether roles, responsibilities and competencies for BCM had been established, 10% said to no extent at all, 30% to a small extent, 34% to moderate extent, 18% to a large extent and no one believed these were established to a very large extent. 8% did not respond to this question. This confirms KEBS' leadership and top management commitment. Establishment of roles, responsibilities and competencies are done and supported by top management.

According to 16% of respondents, persons responsible and accountable for the implementation of the BCMS had not been appointed, while 24% believed to a small extent, 34% to moderate extent, 12% to a large extent and 14% to a very large extent that these persons had been appointed. This results in a total of 84% of the respondents believing that persons responsible for the implementation and maintenance of the BCMS at KEBS had been appointed.

Criteria for accepting risks and the acceptable levels of risk were not defined according to 12% of the respondents, while 32% believed these were defined to a small extent, 38% to moderate extent, 12% to a large extent, and 6% believed these were defined to a very large extent. A total of 88% of respondents believed, though to varied extents, that these criteria and levels were defined at KEBS. Table 4.3 shows the extent of the staff's perception of KEBS' leadership and top management commitment towards the implementation of the BCMS.

On average, 14% of the respondents did not believe that there was leadership and top management commitment to the implementation of a BCMS at KEBS. Commitment to a small extent was perceived by 28% of the respondents, while 32% perceived moderate extent, 18% a large extent, and 6% believed the commitment was there to a very large extent. On average, 2% of respondents did not respond to questions. These overall results are illustrated in Figure 4.3.

Table 4.3 Leadership and Top Management commitment to BCMS at KEBS (responses in %)

1 = No extent at all, 2 = To a small extent, 3 = Moderate extent, 4 = Large extent, 5 = Very large extent

No.		**1**	**2**	**3**	**4**	**5**	**No response**
1	Strategic Policies and objectives for the BCMS are established.	8	22	40	24	6	0
2	BCMS requirements are integrated into business processes.	10	18	38	26	6	2
3	Resources for BCMS are allocated and available.	20	32	32	8	4	4
4	Importance of effective BCM and conforming to the BCMS requirements is well communicated.	16	36	24	20	4	0
5	Direction and support for effectiveness of the BCMS are provided to relevant management roles.	8	36	30	16	10	0
6	Continual improvement is promoted	14	16	34	26	6	4
7	A business continuity policy is available communicated and reviewed.	26	34	20	18	0	2
8	BCMS objectives and plans are established.	14	26	34	18	8	0
9	Roles, responsibilities, and competencies for BCM established.	10	30	34	18	0	8
10	Person(s) responsible for the BCMS with the appropriate authority and Competencies, accountable for the implementation and maintenance of the BCMS are appointed.	16	24	34	12	14	0
11	Criteria for accepting risks and the acceptable levels of risk are defined.	12	32	38	12	6	0
	Average Top Management Commitment	**14**	**28**	**32**	**18**	**6**	**2**

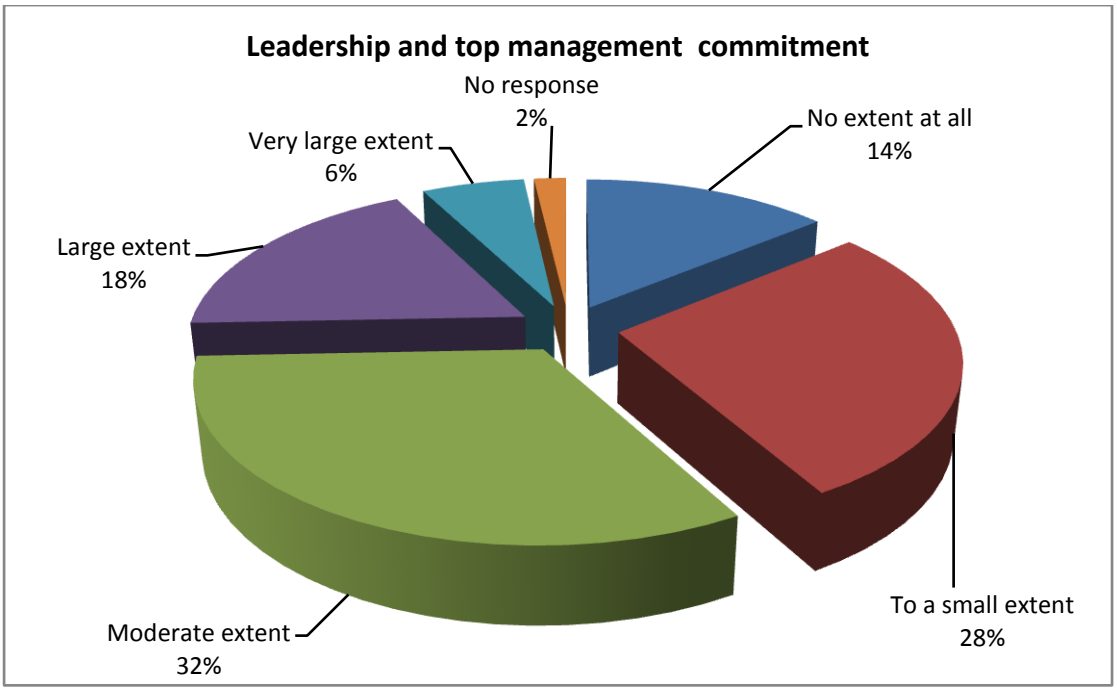

Figure 4.3 Overall leadership and top management commitment for the BCMS implementation at KEBS

4.2.4 Operational Requirements

Questions posed in this section sought to find out the extent to which the following operational requirements of the BCMS are applied at KEBS. Respondents were asked to indicate their perceived extent of these applications on a scale from 1 to 5, where 1 = no extent at all, 2 = small extent, 3 = moderate extent, 4 = large extent, and 5 = very large extent.

Asked whether an evaluation process for determining continuity and recovery priorities, objectives and targets had been established and documented, 12% of the respondents indicated no, 32% to a small extent, 30% to a moderate extent, 24% to a large extent and 2% to a very large extent. This shows that 88% of the total respondents agreed that this operational requirement is in place at KEBS.

The impacts of disrupting activities are not assessed according to 8% of the respondents, while 28% replied that these impacts are assessed to a small extent, 34% to a moderate extent, 20% to a large extent and 8% to a very large extent. However, 2% did not pick any option, which is an indication that they were not aware of this

operational requirement. These answers show that close to 90% of the respondents were aware of this operational requirement, and affirm of its implementation at KEBS.

Asked whether a formal documented risk assessment process had been established, implemented and is being maintained, 10% said no, while the majority of 38% said to a moderate extent, 22% to a small extent, 24% to a large and 6% to a very large extent. Generally, 90% of the respondents affirmed, to varied levels of extent, that KEBS has put this operational requirement in place.

A large proportion of 44% of the respondents affirmed to a moderate extent that strategies from the business impact analysis and risk assessment had been determined and selected, while 14% claimed that not being the case. Further, 28%, 8% and 6% affirmed to a small extent, large extent and very large extent, respectively, that such strategies had been determined and selected. Overall, 86% of the respondents agreed to varied extents that this operational requirement is applied at KEBS.

The determination of resource requirements for implementing the selected strategies was affirmed by 40% of the respondents to a moderate extent, by 18% to a small extent, by 22% to a large extent and 2% to a very large extent. It was noted that only 14% claimed that this requirement was not met at KEBS, and 4% of the respondents were not aware of this operational requirement. The majority of 82% of respondents agreed that this operational requirement is applied at KEBS.

Asked whether risks requiring treatment are identified, 10% of the respondents indicated no identification at all, 20% to a small extent, 42% to a moderate extent, 16% to a large extent, 10% to a very large extent and 2% did not indicate any option. These responses indicate that a solid majority of respondents (88%) is aware of the identification of risks requiring treatment at KEBS.

When respondents were asked whether business continuity procedures had been established, implemented and are being maintained, 18% indicated no, 20% to a small extent, 36% to a moderate extent, 20% to a large extent and 6% to a very large extent. These replies indicate that there is still a lack of communicating these procedures to many staff members at KEBS.

Asked about the establishment, implementation, maintenance and regular exercise of procedures for warning and communication, it was found that 20% of the respondents indicated no extent of awareness at all, 26% to a small extent, 24% to a moderate extent, 18% to a large extent, 10% to a very large extent and 2% did not reply. Almost half of the respondents (48%) were not, or only to a small extent, aware of the procedures for warning and communication. This indicates a significant lack in the application of this operational requirement at KEBS.

Queried whether business continuity procedures being exercised and tested, 24% of the respondents said this does not happen at all, 30% to a small extent, 32% to a moderate extent, 12% to a large extent and 2% to a very large extent. This shows that there is very little awareness on exercise and/or testing of BC procedures at KEBS. There is need for improvement in this area because exercising and testing are critical aspects in validating business continuity plans and procedures. The evidenced lack of awareness about their existence is a sign of lacking preparedness to respond and recover within agreed timelines.

The requirement for documented procedures for responding to a disruptive incident being in place was not applied according to 20% of the respondents, while 28% indicated to a small extent, 34% to a moderate extent, 14% to a large extent and 4% to a very large extent. These responses indicate that the majority of the respondents (80%) are aware of such documented procedures at KEBS, even though 28% were only to a small extent aware of them.

Asked whether documented procedures for restoring and returning business activities from temporary to normal business requirements after an incident have been established, it was found that 16% of the respondents said this did not happen at all, while 34% claimed the establishment of such procedures to a small extent, 30% to a moderate extent and 20% to a large extent. This means that one-half of the respondents are either not, or only to a small extent, aware of the procedures to return to normal business requirements after an incident at KEBS, indicating the lack of proper communication of such procedures to all staff members.

Many members of staff at KEBS do not seem to be aware of BC procedures, procedures for warning and communication, procedures for responding to a disruptive

incident, procedures to restore and return business activities from temporary mode, and awareness that the procedures are exercised and tested, attracting the highest percentage not believing they exist at all, at 18%, 20%, 20%, 16% and 24%, respectively.

The answers of all respondents to the operational requirements of the BCMS are summarized in Table 4.4.

Table 4.4 Operational Requirements of the BCMS applied at KEBS (responses in %)

1= No extent at all 2= To a small extent, 3= Moderate extent 4= Large extent 5= Very large extent

No.		**1**	**2**	**3**	**4**	**5**	**Not indicated**
1	Evaluation process for determining continuity and recovery priorities, objectives and targets are established and documented.	12	32	30	24	2	
3	Impacts of disrupting activities are assessed.	8	28	34	20	8	2
4	A formal documented risk assessment process is established, implemented and maintained.	10	22	38	24	6	
5	Strategy from the business impact analysis and risk assessment are determined and selected.	14	28	44	8	6	
6	Resource requirements to implement the selected strategies are determined.	14	18	40	22	2	4
7	Risks requiring treatment are identified.	10	20	42	16	10	2
8	Business continuity procedures established, implemented and maintained.	18	20	36	20	6	
9	Procedures for warning and communication which are regularly exercised are established, implemented and maintained.	20	26	24	18	10	2
10	Documented procedures for responding to a disruptive incident are established.	20	28	34	14	4	

11	Documented procedures to restore and return business activities from the temporary to support normal business requirements after an incident are established.	16	34	30	20	-	
12	Business continuity procedures are exercised and tested.	24	30	32	12	2	

4.2.5 Major Threats to the Business Continuity at KEBS

The level of awareness towards major threats to BC at KEBS was investigated. Respondents were asked to identify major BC threats to KEBS from a list of 25 potential threats, by indicating each one with "yes" (major threat) or "no" (not a major threat to KEBS' BC). The questionnaire also provided a space to fill in another major threat manually, but no additional ones were offered by the respondents.

Unplanned IT Outages were identified as a major threat by 82% of the respondents, indicating high awareness towards this threat. The threats of a Business Ethics Incident and Data Breach were each identified by 76%, followed by a Cyber Attack by 70% of the respondents. Scarcity of Natural Resources was indicated least frequently, by only 22% of the respondents, followed by Energy Cost at 28% and then Key Customer Insolvency at 34%. Looking at the proportion of the respondents who did not indicate whether they were aware of threats or not, it was found that of the 25 threats, this proportion ranged from 6% for cyber-attack to 34% for energy availability. This indicates that many respondents are not aware that these incidents can pose threats to the BC at KEBS. All responses are represented in Figure 4.4.

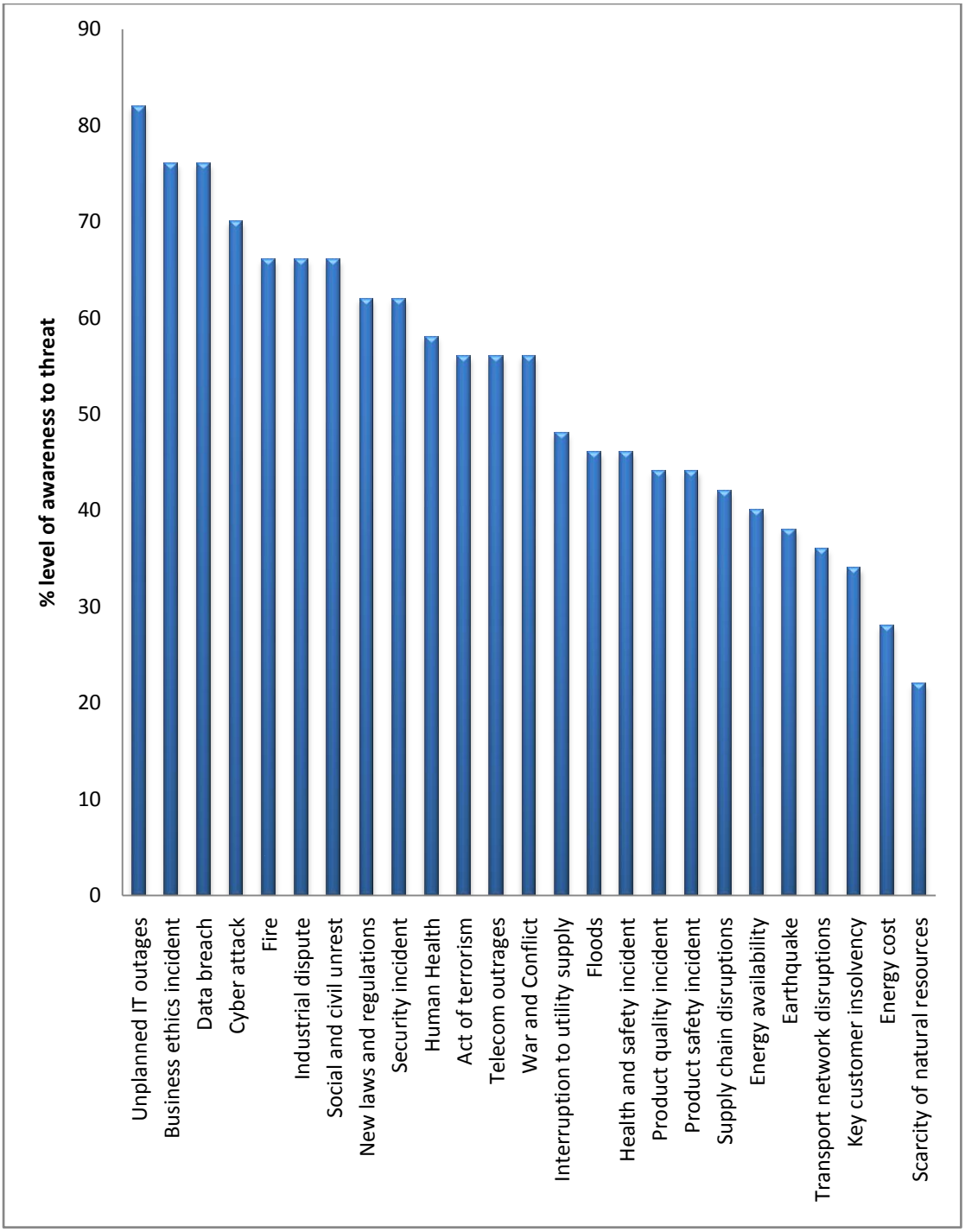

Figure 4.4 Major threats to BC at KEBS

4.2.6 Hurdles to BCMS/BCM Implementation at KEBS

To investigate the hurdles, which the implementation of the BCMS at KEBS faces, 14 challenges were identified and respondents were asked to rate the extent to which each challenge presents a hurdle to BCMS implementation based on a Likert scale from 1 to 5, where 1 = no extent at all, 2 = to a small extent, 3 = to a moderate extent, 4 = to a large extent, and 5 = to a very large extent. The average percentage to varying extents was found by adding figures for a small extent, moderate, large and very large extent.

Analysis of the respondents' answers indicates that lack of senior management support is seen as the biggest challenge to the implementation of the BCMS at KEBS (94% of the respondents believe so, with 44% considering it a challenge to a very large extent, 24% to a large extent, 20% to a moderate extent and 6% to a small extent).

Government interference, bureaucracy and corruption were observed as posing other major challenges to the implementation of the BCMS, all with 92% of the respondents indicating these. 8% and 6% of the respondents, respectively, did not give any response on bureaucracy and corruption. Government interference was voted as a major challenge in the implementation of the BCMS with 52% of the respondents indicating it to a very large extent, 24% to a large extent, 6% to a small extent and 10% to a moderate extent. 8% did not respond on this threat and none answered no extent at all.

On the same note, bureaucracy shared the second highest percentage (92%) of respondents, 34% indicating it to a very large extent, 22% to a large extent, 28% to a moderate extent and 8% to a small extent as challenge to the implementation of the BCMS at KEBS. Other challenges included poor supervisory, also with 92% of the respondents in varying level of extents confirming.

Procurement delays were also a major challenge with only 2% of the respondents indicating that it is not a challenge at all, and 34% indicating it is a challenge to a very large extent, 22% to a large extent and 34 to a moderate extent. This makes 92% of the respondents who identified this as a challenge.

The same percentage of respondents (92%) considers conflict of interest in influential stakeholders a key challenge to the implementation of the BCMS at KEBS.

Another challenge was change of government, which was viewed by only 6% as not being a challenge at, while 36% viewed it as a challenge to a very large extent, 20% to a large extent, 14% to a moderate extent and 16% to a small extent.

The least considered as challenge was a delay in payments with 14% of the respondents indicating it as not being a challenge at all, and 6% not giving any response.

This was followed by a change in project sponsor, and difference in work culture change. These had a proportion of 12% and 10%, respectively, of respondents who did not find them as challenges at all. Similarly, the 8% of respondents in each case who did not provide any response might be an indication that the respondents did not understand these challenges in the light of a BCMS implementation.

Detailed responses are shown in Table 4.5.

Table 4.5 Summary of the challenges in implementation of BCMS (responses in %)

1 = No extent at all, 2 = To a small extent, 3 = Moderate extent, 4 = Large extent, 5 = Very large extent.

Challenges	**1**	**2**	**3**	**4**	**5**	**No response**
Change of Project Sponsor	12	18	24	14	24	8
Change of Government	6	16	14	20	36	8
Difference in Work Culture Change	10	24	30	20	8	8
Conflict of interest in influential project stakeholders	4	14	18	32	28	4
Lack of senior management support	4	6	20	24	44	2
Identification of right stakeholders	2	26	18	24	18	12

Business reengineering challenges	4	20	22	26	20	8
Delay in Payments	14	14	26	26	14	6
Bureaucracy	0	8	28	28	34	8
Government Interference	0	6	10	24	52	8
Procurement delays	2	2	34	22	34	6
Corruption	0	6	30	30	28	6
Incomplete requirements	6	12	22	40	16	4
Poor supervisory	2	14	28	20	30	6

CHAPTER FIVE: SUMMARY OF THE FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter summarizes the findings, provides conclusions and recommendations based on the objectives of this study. The objective of this study was to evaluate the implementation of the Business Continuity Management System (BCMS) at the Kenya Bureau of Standards (KEBS). Three areas were evaluated: context of the organization, leadership commitment, and operational requirements. Data was collected by questionnaire from KEBS staff members at four different organizational levels top management, department heads, technical staff, and non-technical staff.

5.2 Summary of Findings

In the context of the organization, the study found that overall 51% of the respondents believed systems addressing the context of KEBS were in place, 43% believed these systems were not in place, and 6% did not provide an answer. A majority of 72% of respondents agreed that links of objectives, policies and risk management strategy are identified and documented. This difference could be attributed to the fact that many employees at KEBS are generally aware of risk management because it forms part of the staff performance evaluation. This circumstance may have influenced the 21% difference in the respondents' positive responses. Respondents agreed to 68% that KEBS' functions, products and the impact of disruptive incidents are identified and documented. This high level of positive responses could reflect the fact that for any BCMS to be set up, it is a pre-requisite to identify and document the organization's functions, products and impact of disruptive incidents. This follows ISO 22301 requirements. Awareness of the definition of the BCMS scored lowest, together with the definition of the uncertainty that gives rise to risk, yet these are two very critical components for the implementation of the BCMS. According to (Hiles, 2007), an organization's risk appetite is a definition of each level of risk which it is prepared or able to accept. KEBS scored low on this according to 56% of respondents who disagreed that risk appetite had been identified and documented. These results clearly demonstrate that the awareness level on the existence of the documentation on the BCMS is low at KEBS. The overall level of awareness towards existing systems that comprise the context of the organization was found to be at 51%. This might be due to

the fact that the BCMS is still new at KEBS and organization-wide awareness through audits has not yet been raised.

The evaluation of KEBS' leadership and top management commitment revealed that only 16% of the respondents were unsure about or doubted the commitment by the leadership, while 84% believed there was top management commitment. An overwhelming majority of respondents (92%) believe that KEBS' top management had established strategic policies and objectives, as well as providing direction and support for the effectiveness of the BCMS. This reflects well the necessity that any system implementation requires top management commitment. Leadership and top management commitment is also considered as one of the Total Quality Management (TQM) principles.

KEBS has trained a limited number of staff members on the BCMS and has plans to become certified against the BCMS standard ISO 22301:2012. BCMS policy was in place at KEBS according to 72% of respondents. These positive responses are another sign of top management commitment to BCMS implementation at KEBS. Other systems were already in place before the BCMS implementation started, especially the risk management system, which most respondents identified as being part of BCMS. Overall, top management commitment was shown to be strongly present at KEBS, which is important to successfully implement this system.

On operational requirements, 24% of the respondents believed that no BC procedures were exercised and tested. Further, 20% of the respondents believed there were no procedures for warning and communication. These results are consistent with the fact that without well-established systems, which are communicated throughout the organization, implementation of a BCMS becomes very difficult and will be unsuccessful. The study results indicate a low awareness level by KEBS employees of the operational requirements being met by KEBS to address BC.

As far as major threats to BC are concerned, unplanned IT outages led with 82% of the respondents indicating this as a threat, followed by data breach and business ethics incident at 76% each. KEBS relies on Information Technology for most of its operations, and disruptions to IT would compromise effective service delivery by KEBS to stakeholders, including the public. This is confirmed by the outcome of this

aspect of the study. High adaptive capacity of KEBS is a requirement for business continuity during and after a disruption. The adaptive capacity to these identified threats relies on full implementation of the operational requirements and having systems in place, regarding the context of organization. The success of increasing KEBS' adaptive capacity can be achieved through full support by the top management in terms of resource availability, policy formulations, trainings and allocation of duties and responsibilities, among others.

The biggest challenge in the implementation of the BCMS at KEBS was shown to be lack of senior management support (indicated by 94% of the respondents), which would be expected to be the same in other organizations as well. The positive responses on the commitment of KEBS' top management (as shown above), seem to indicate that KEBS is successfully on its way to overcome this challenge. Bureaucracy, government interference, procurement delays and poor supervisory, were all named as second biggest challenges by 92% of the respondents. Government interference and lack of senior management commitment were perceived to pose the biggest challenges to BCMS implementation by 52% and 44% of respondents, respectively, indicating these as having a very large extent of influence.

5.3 Conclusion

This study concludes that KEBS has implemented its BCMS but overall awareness amongst the staff members is too low for a working system at 51.4%. It is evident that the system has not been communicated to staff members very well. Systems are believed to be in place as far as BCMS is concerned and procedures seem to be available but these do not seem to have been exercised and tested at an acceptable level.

The study also concludes that employees at KEBS are more familiar with risk management than the BCMS and that they believe the biggest threats to BC are unplanned IT outages. KEBS employees consider government interference as a major challenge to the implementation of the BCMS. KEBS has its BCMS in place but full implementation is still low, the existence of many systems is only known to a limited number of staff members. The awareness among staff of this BCMS is also low due to the lack of organization-wide exercise and testing programs or procedures for BC. KEBS' top management seems committed to the BCMS as evidenced in the average

of 82% of respondents who believe there is such commitment and only 14% not believing in this commitment.

In summary, KEBS has systems in place as far as organizational context is concerned. Operational requirements are also met, though not completely, and the need for staff training and better communication is evident. A major threat to BC at KEBS was identified as unplanned IT outages. While lack of senior management support, together with government interference, were identified as the major challenges to the full implementation of the BCMS at KEBS, a strong commitment by senior management towards the BCMS implementation has also been shown.

5.4 Recommendation

The findings of the study indicate that implementation of BCMS is still not a whole-organization affair as far as the three requirements are concerned, i.e. context of organization, leadership and top management commitment and operational requirements. This study recommends BCMS awareness creation throughout KEBS. This need is supported by (Ian, 2009) that successful business continuity management requires a commitment from the executive to raising awareness and implementing sound approaches to build resilience.

Operational requirements were moderately being implemented according to a large percentage of KEBS staff. This calls for KEBS to ensure these requirements are fully implemented, communicated and procedures fully exercised and tested. Through implementation of operational requirements, KEBS will be in a position to identify its key vulnerabilities and develop strategies on how to mitigate them. Full implementation of the operational requirements would also raise KEBS' adaptive capacity since procedures would be exercised and tested to ascertain readiness in responding to disruptions and restoring operations to the acceptable level within the agreed timeline. KEBS needs to develop measures for addressing unplanned IT outages, data breaches, security incidences, handling of business ethics incidences and other risks it is exposed to. The full implementation of the holistic BCMS throughout the organization will provide a means of identifying and addressing these threats to KEBS and therefore would give KEBS a higher adaptive capacity in case of disruptions.

The study also recommends that the government be aware of the challenges KEBS faces on their way to successful implementation of BCMS/BCM, and come up with ways to mitigate these challenges. These challenges include government interference, corruption and change in government. KEBS top management is seen to be committed to full support of BCMS and this commitment is recommended for continual improvement. Leadership and Top management commitment is seen as a threat to BC.

The study recommends that the government of Kenya should have regulations in place to accommodate the need for BCMS in government organizations since regulations and guidelines are an excellent approach in ensuring completeness and compliance with best practice. This will make sure all government institutions are BCMS certified to safeguard the government's investments/resources. Recommendation also goes to Insurance companies to consider products that reflect BCMS implementation.

KEBS dependance on the government and the challenge government interference may pose on KEBS BC requires an operational strategy that BCMS provides.

5.5 Recommendation for Further Research

This study has evaluated the implementation of BCMS at KEBS. It is therefore recommended that further research be done in other parastatals and government bodies on implementation of BCMS. It is also recommended that research be done covering the remaining requirements of BCMS at KEBS, which include planning, support, performance evaluation and improvement of BCMS.

REFERENCES

BSI Group. (2014, May). *BSI whitepaper for Business: Beyond Recovery, The broader benefits of Business Continuity Management*. Retrieved May 27, 2014, from BSI Website: www.bsigroup.com/en-GB/iso-22301-business-continuity/business-continuity-awareness-week/

Business Continuity Institute in association with BSI. (2014). *Horizon Scan.* United Kingdom: Business Continuity Institute.

CDC. (2011). *CDC Estimates of 2009 H1N1 influenza cases, hospitalization and deaths in the USA.* Atlanta: CDC.

CDP. (2014, May 26). *A review of findings from CDP 2011-2013 disclosures.* Retrieved May 27, 2014, from Continuity Central Website: https://www.cdp.net/CDPResults/review-2011-2013-USA-disclosures.pdf

Ernest&Young. (2012). *Ready for the challenge-Integrated governance:The key to effective BCM.* London: EYGM Limited.

Hiles, A. (2007). *The definitive handbook of business continuity management, seconf edition.* West Sussex: John Wiley & Sons Ltd.

Hugh, M. (2010). *Business Continuity management and the Healthcare Center.* London: MARSH Ltd.

Ian, M. (2009). *BCM Buiding Resilience in Public Sector Entities.* Australian National Audit Office.

Ihab, H. S., Sawalha, J. R., & Anchor, J. M. (2012). Business Continuity Management in Jordanian Banks: Some cultural considerations. *Risk Management*, 5-6.

Insurance, V. R. (2012). *Understanding Business Continuity Management.* VMIA.

International Organisation for Standardization. (2012). *ISO 22301*. Geneva: ISO.

ISO. (2012). *Societal Security- Business Continuity Management Systems-Guidance.* Switzerland: ISO Copyright Office.

Kothari, C., & Garg, G. (2014). *Research Methodology-Methods and Techniques.* New Delhi: New age international Ltd publishers.

Mathenge, M. W. (2011). *Disaster Recovery and Business Continuity Plans in Class A Parastatals in Kenya.* Nairobi: University of Nairobi Press.

Metzler, D. J. (2014, June 2). *Business continuity and disaster recovery planning*. Retrieved from Storage special report: http://www.ashtonmetzler.com/BizContDisRec_FINALl.pdf

Ministry of State for Special Programmes. (2013). *National Progress Report on Implementation report on Hyogo Framework for Action 2011-2013.* Nairobi: PreventionWeb.

NSW. (2005). *Business Continuity-Management Recovery Plan 2010-2015.* Sydney: NSW Government.

Pearson, G., & Woodman, P. (2012). *Planning for the worst.* London: Chartered Management Institute.

Porter, M. E. (1985). Competitive Advantage: Creating and Sustaining Superior performance. In M. E. Porter, *Competitive Advantage: Creating and Sustaining Superior performance* (p. 34). New York: Free Press London:Collier Macillan.

Regina Below, A. W.-S. (2009). *Disaster Category Classification and Peril terminology for operational purposes.* Brussels: CRED and MUNICH RE.

Resilience Development Initiative. (2014). *Climate Change Policy Development in Indonesia.* Bandung: Indonesia Climate Change Trust Fund.

RSA-ARCHER. (2012). *Business Continuity Management and Operations.* USA: EMC Corporation.

Shivo, J. L. (2010). *Business Continuity Planning- The case of Agricultural Research Institutions in Kenya.* Nairobi, Kenya.: University of Nairobi Press.

ST-Germain, R., Aliu, F., Lachapele, E., & Dewez, P. (2012). *Whitepaper on Societal Security Business Continuity Management System.* New York: PECB ISO 22301.

Systems on Silicon Manufacturing Company Pte Ltd. (2014, August 23). Emerging Unscathed from the Japan Earthquake and Tsunami. *Emerging Unscathed from the Japan Earthquake and Tsunami*, Retrieved from Emerging Unscathed from the Japan Earthquake and Tsunami: http://www.bcm.org.sg/Portals/2/CaseStudies/SSMC%20BCM%20Article.pdf

UNISDR. (2014, March 24). *PreventionWeb*. Retrieved from Ministry of Special ProgramsWebsite:www.preventionweb.net/english/professional/contacts/profile.php?id=8898

VMIA. (2012). *Understanding Business Continuity Management.* VMIA.

WauchopeMC. (2011). *Business Continuity Management Guidelines.* Western Australia: Insurance Commission of Western Australian.

Whitehorn, G. (2010). Building Organisational Resilience in the public sector. *Comcover Insurance and Risk Management Conference* (pp. 1-20). Canberra: National Portrait Gallery.

Woodman, P., & Hutchings, P. (2010). *Disruption and Resilience.* London: Chartered Management Institute.

Zawada, B., & J, S. (2003). BCM standard a side by side comparison. *Information systems control journal vol 2*.

APPENDICES

APPENDIX I: QUESTIONNAIRE

BUSINESS CONTINUITY MANAGEMENT SYSTEM IMPLEMENTATION

This questionnaire has been designed to assist the researcher collect data concerning Business Continuity management system Implementation at Kenya Bureau of Standards. You have been identified as one of the respondents in this study. Section A: contains questions on respondent profile, Section B: Context of Organization (KEBS), Section C- leadership and top management commitment, Section D- Operational requirements for BCMS, Section E- The major threat(s) to Business Continuity and Section F- Challenges in implementing BCMS/BCM. The information collected will be used for academic, policy and research purposes only and confidentiality is highly assured.

SECTION A: Respondent Profile

Please provide information by ticking in the appropriate boxes [ ].

1. What is your designation in the organization?

CEO/MD [ ] Management Representative [ ]

IT Manager [ ] Business Analyst/Strategist [ ]

Network & Sys Admin [ ] Operations Manager [ ]

Others (please specify…….....)

2. How long have you worked at KEBS?

[ ] 1-10 years [ ] 11-20 [ ] 21-30 [ ] 31 years and above

Section B: Context of the organization

Have the following aspects of organizational context been established? Please tick appropriately.

No		Yes	No
1	Functions and products and impact of disruptive incident are identified and documented.		
2	Links of objectives, policies and risk management strategy identified and documented.		
3	Risk appetite identified and documented		
4	Business Continuity objectives articulated.		
5	Uncertainty that gives rise to risk are defined		
6	Risk criteria taking into account the risk appetite is set.		
7	Purpose of the BCMS is defined		
8	Interested parties relevant to BCMS and their requirements are determined.		
9	Procedures to identify, access and assess applicable legal and regulatory requirements related to continuity of operations are available.		
10	Scope, mission, goals of BCMS established		

Section C- Leadership and top management commitment: To what extent have the following been demonstrated by leadership in the organization? Please tick appropriately, where:-

1= No extent at all 2= To a small extent, 3= Moderate extent 4= Large extent 5= Very large extent

No.		1	2	3	4	5
1	Strategic Policies and objectives for the BCMS are established.					
2	BCMS requirements are integrated into business processes.					
3	Resources for BCMS are allocated and available.					
4	Importance of effective BCM and conforming to the BCMS requirements is well communicated.					
5	Direction and support for effectiveness of the BCMS are provided to relevant management roles.					
6	Continual improvement is promoted					
7	A business continuity policy is available communicated and reviewed.					
8	BCMS objectives and plans are established.					
9	Roles, responsibilities, and competencies for BCM established.					
10	Person(s) responsible for the BCMS with the appropriate authority and Competencies, accountable for the implementation and maintenance of the BCMS are appointed.					
11	Criteria for accepting risks and the acceptable levels of risk are defined.					

Section D:-Operational requirements: To what extent have the following been applied in the organization? Please tick appropriately, where:-

1= No extent at all 2= To a small extent, 3= Moderate extent 4= Large extent 5= Very large extent

No.		1	2	3	4	5
1	Evaluation process for determining continuity and recovery priorities, objectives and targets are established and documented.					
3	Impacts of disrupting activities are assessed.					
4	A formal documented risk assessment process is established, implemented and maintained.					
5	Strategy from the business impact analysis and risk assessment are determined and selected.					
6	Resource requirements to implement the selected strategies are determined.					
7	Risks requiring treatment are identified.					
8	Business continuity procedures established, implemented and maintained.					
9	Procedures for warning and communication which are regularly exercised are established, implemented and maintained.					
10	Documented procedures for responding to a disruptive incident are established.					
11	Documented procedures to restore and return business activities from the temporaryto support normal business requirements after an incident are established.					
12	Business continuity procedures are exercised and tested.					

Section E:- Which of the following do you consider as the major threat to business continuity in your organization. Please tick appropriately.

		Yes	No
1.	Unplanned IT outages		
2.	Telecom outages		
3.	Cyber attack		
4.	Data breach		
5.	Security incident		
6.	Fire		
7.	Interruption to utility supply		
8.	Health and safety incident		
9.	Act of terrorism		
10.	Energy cost		
11.	Energy availability		
12.	Product safety incident		
13.	Key customer insolvency		
14.	Scarcity of natural resources		
15.	Earthquake		
16.	Floods		
17.	Transport network disruptions		
18.	New laws and regulations		
19.	Human Health		
20.	Supply chain disruptions		
21.	Product quality incident		
22.	War and Conflict		
23.	Industrial dispute		
24.	Social and civil unrest		
25.	Business ethics incident		

Other----------

Section F:- Which of the following would you consider as challenges in implementation of BCMS/BCM. Please tick appropriately where:-

1= No extent at all 2= To a small extent, 3= Moderate extent 4= Large extent 5= Very large extent

		1	2	3	4	5
1.	Change of Project Sponsor					
2.	Change of Government					
3.	Difference in Work Culture Change					
4.	Conflict of interest in influential project stakeholders					
5.	Lack of senior management support					
6.	Identification of right stakeholders					
7.	Business reengineering challenges					
8.	Delay in Payments					
9.	Bureaucracy					
10.	Government Interference					
11.	Procurement delays					
12.	Corruption					
13.	Incomplete requirements					
14.	Poor supervisory					

Other----------

