DISASTER RECOVERY AND BUSINESS CONTINUITY PLANS IN CLASS-A PARASTATALS IN KENYA

BY

NAMES: MICHAEL WANDERI MATHENGE

A MANAGEMENT RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION, SCHOOL OF BUSINESS, UNIVERSITY OF NAIROBI

OCTOBER, 2011

STUDENT'S DECLARATION

I, the undersigned, declare that this is my original work and has not been submitted to any other college, institution or university other than the University of Nairobi for academic credit.

Signed: _____ Date: _____

Michael Wanderi Mathenge (D61/P/7113/05)

This project has been presented for examination with my approval as the appointed Supervisor.

Signed: _____ Date: _____

Dr. Kate Litondo

DEDICATION

This study is dedicated to my loving family and fiancée for their endless support. Their encouragement has helped me get to where I am.

ACKNOWLEDGEMENT

I thank the Almighty God for His guidance and providence which enabled me to undertake this project that was too involving in terms of time and resources.

I wish to express my sincere appreciation to my family for their understanding and support during the project.

I would like to express my sincere thanks to the moderator Mr Joel Lilei for having agreed to moderate this research paper and his patience in reading the drafts and occasionally guiding me.

Lastly, I would also like to express my sincere thanks to my supervisor Dr. Kate Litondo for having agreed to supervise this research paper and her patience in reading the drafts and occasionally guiding me, without which the research would not have been a reality.

ABSTRACT

Information has almost single handedly become one of the most critical success factors for most organizations. Through the use of vast information bases organizations are able to make relevant and important strategic, tactical and operational decisions that give them a competitive edge. The continued operations of an organization depends to a large extent on management's awareness of potential disasters, their ability to develop plans to minimize disruptions of critical functions and the ability to conduct recovery operations successfully with the least amount of downtime. Business Continuity Planning (BCP) is defined as a proactive planning process that ensures critical services or products are delivered during a disruption while Disaster Recovery (DR) can be defined as the process by which you resume business after a disruptive event. A disaster can therefore be defined as the loss or interruption of a critical service(s) or process for a period of time which threatens the ability of the enterprise to fulfill its mission. The general objectives of this study were to assess the disaster recovery and business continuity plans of class-A parastatals in the various government ministries.

Research design employed in this study is descriptive in nature. The study focused on Class A parastatals as they represent huge government corporations both in-terms of strategic importance, revenue and employees. This study employed a survey method of design. The study targeted 54 senior and middle-level management employees. Primary data was collected using self-administered questionnaires. The data collected from this study was mainly presented through the use of summarized percentages, proportions and tabulations and other data presentation tools in all the sections of the questionnaires.

The study concludes that during pre-planning consulting business process owners during the business impact assessment was considered the most important step. During plan development, developing a formal system backup policy and schedule was most important while during testing having frequently scheduled tests was most important. Establishing agreements with critical vendors' and service providers was considered most important in plan maintenance. The greatest benefit of implementing BC and DR was reduced downtimes while the greatest challenge in implementation was beauracracy. The

study concludes that parastatals should invest in BCP and DR in order to minimize downtimes as well as safeguard their information.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE: INTRODUCTION

1.1 Background to the Problem

Kenya has been moving very rapidly towards embracing Information, Communication and Technology (ICT) as a means to growth and efficient service delivery to the citizenry. With the rapid growth and the subsequent adoption of information technology as a competitive tool in Parastatals and other organizations so has the threat from internal and external attacks on IT systems and data increased. According to Nalo (2007) the role of ICT in vision 2030 is categorized as an enabler of business both in government and private sector by improving internet access, developing strategies to improve access to ICT by decreasing cost of business as well as reducing the cost of communication, management and transaction of data. He further classifies ICT enablers as education, skills training, research and development, access to venture capital, affordability of Internet access, security of Internet infrastructure, Government support for ICT development, and quality of ICT supporting services. This therefore means that the role of ICT in Kenya and the reliance on ICT by both government and private sector is increasing rapidly and thus the need to protect the vital information and data held by the various information systems.

With the increased dependency of on-line applications, Internet usage and up-to-date information to facilitate decision-making and run daily operations, business processes and their support systems require continuous availability. Regardless of how well you build redundancies into the infrastructure, such as, UPS, generators, hardware replication or how well you try to shield yourself from the hackers and crackers of the world, there will always be those natural and man-made disasters that can have a devastating impact on the organization. Information has, almost single handedly become one of the most critical success factors for most organizations. The value of this information can therefore not be emphasized enough. Through the use of vast information bases, organizations are able to make relevant and important strategic, tactical and operational decisions that give them a competitive edge. The continued operations of an organization depends to a large extent on management's awareness of potential disasters, their ability to develop plans to

minimize disruptions of critical functions and the ability to conduct recovery operations successfully with the least amount of downtime.

According to a report by the Federal Office for Information Security (2009), Government agencies and companies are exposed more and more to risks that endanger productivity or the ability to provide their services to their customers promptly and continuously. Various developments and trends in society and the economy contribute to these risks, for example increasing globalization, networking, centralization, automation, outsourcing, or off-shoring. Due to the increasing complexity of business processes and their rising dependency on information technology and external service providers, events such as fires, floods, or the loss of information technology, service providers, suppliers, or personnel can have a significant impact. Furthermore, the risk of pandemics, extreme weather conditions, and terrorism is also increasing.

A Gartner Research (2001) established that in the aftermath of recent natural disasters, terrorism, and equipment breakdown, businesses have recognized more than ever the need for an organization to be prepared. Companies are striving to meet the demand for continuous service. With the growth of e-commerce and other factors driving system availability expectations toward 24x365, the average organization's requirement for recovery time from a major system outage now ranges between 2 and 24 hours. This requirement is pushed by the expectation an organization faces on all sides. Some of these include customers' expectations that supplies and services will continue— or resume rapidly— in all situations, shareholders expect management control to remain operational through any crisis, employees expect both their lives and livelihoods to be protected, suppliers expect their revenue streams to continue in at least the short term, regulatory agencies expect their requirements to be met, regardless of circumstances, and insurance companies expect due care to be exercised.

Closer home, my personal experience during a disaster has been two fold. I once had to recover an email server when the email server for the company I work for crushed. This was a trying moment as we virtually lost all employees emails as we did not have any backups in place. In the recent past our (Enterprise Resource Planning) ERP server

crushed. This time round we were fortunate enough that we had backups that work. Both of these experiences have helped shape my interest in DR and BCP due to the disruptive nature of the incidents.

1.1.1 Types of Disasters

The following relate to some of the disasters that an organization ought to consider when implementing disaster recovery mechanisms. These hazards are contextualized to the Kenyan climatic condition and hence do not encompass all hazards that would be found in other parts of the world. Some of them include natural disasters which can include earth quake disasters, environmental disasters, weather disasters, fire disasters, tsunamis, floods, lightning, freezing temperatures, fallen trees, chemical spills, biological attack, and severe hail storms. Others are manmade disasters which are caused by people deliberately and negligently causing disasters all over the world. Some of these include bomb attacks, disruption of communications, interruption in shipments, destruction of records and production equipment are all ordinary results of manmade disasters and a prudent business will prepare for their occurrence. The final one is customer defined disasters which include customer specific disasters that have the potential to devastate their business. power loss, excess temperatures, broken plumbing, felled trees, loss of communications, utility failure, work stoppage, deliberate disruption, loss of utilities, loss of supplies, equipment failure, loss of key supplier, loss of key vendor, intentional damage and destruction.

1.1.2 Business Continuity and Disaster Recovery

According to Slater (2010) all Business Continuity (BC) and Disaster Recovery (DR) plans need to encompass how employees will communicate, where they will go and how they will keep doing their jobs. The details can vary greatly, depending on the size and scope of a company and the way it does business. Business continuity is defined as a comprehensive managed effort to prioritize key business processes, identify significant threats to normal operation, and plan mitigation strategies to ensure effective and

efficient organizational response to the challenges that emerge during and after a crisis. Business continuity planning is a proactive planning process that ensures critical services or products are delivered during a disruption. A business continuity plan includes plans, measures and arrangements to ensure the continuous delivery of critical services and products, which permits the organization to recover its facility, data and assets. It also involves identification of necessary resources to support business continuity, including personnel, information, equipment, financial allocations, legal counsel, infrastructure protection and accommodations.

The activities involved include many daily chores such as project management, system backups, change control, and help desk. BC is not something implemented at the time of a disaster; it refers to those activities performed daily to maintain service, consistency, and recoverability. The foundations of BC are the standards, program development, and supporting policies; it also includes guidelines and procedures needed to ensure a firm continues without stoppage, irrespective of the adverse circumstances or events. All system design, implementation, support, and maintenance must be based on this foundation in order to have any hope of achieving Business Continuity, Disaster Recovery, or in some cases, system support. Business continuity is sometimes confused with disaster recovery, but they are separate entities. Disaster recovery is a small subset of business continuity.

According to Slater (2010) Disaster Recovery (DR) can be defined as the process by which you resume business after a disruptive event. The event might be something huge-like an earthquake or the terrorist attacks during the 1997 bomb blast in Nairobi or something small, like malfunctioning software caused by a computer virus. Disaster recovery is a subset of business continuity. DisasterRecovery.org describes disaster recovery as the process an organization uses to recover access to their software, data, and/or hardware that are needed to resume the performance of normal, critical business functions after the event of either a natural disaster or a disaster caused by humans. Defining a disaster is fundamental to business continuity planning. According to Hiles (2003) defining a disaster, escalation procedures and service levels is important as it

enables incidents to be analyzed based on an established criterion. A disaster can also be defined as the loss or interruption of a critical service(s) or process for a period of time which threatens the ability of the enterprise to fulfill its mission. It is also an unanticipated incident or event, including natural catastrophes, technological accidents, or human-caused events, causing widespread destruction, loss, or distress to an organization that may result in significant property damage, multiple injuries, or deaths. In Kenya today parastatals need to take into consideration not just the IT infrastructure but also the work-areas where essential business functions occur. The work-area includes all the needed facilities, such as desks, chairs, telephones, office supplies, and so on. An equally important factor is the human resources factor since for a fact any recovery efforts would fail without having an adequate number of trained personnel on hand to actually perform the critical business functions.

1.1.3 Business Continuity Planning/ Management

The Federal Office for Information Security (2009) defines Business Continuity Management (BCM) as a management process whose goal is to detect serious risks that endanger the survival of an organization early and to implement safeguards against these risks. To a parastatal this basically means that the need to ensure the survival of the company or institution, suitable corrective and/or preventive measures must be taken to increase the availability of the business processes as well as to enable a quick and targeted reaction in case of an emergency or a crisis. Business continuity management consists of a planned and organized procedure for sustainably increasing the availability of real time critical business systems of an organization, reacting appropriately to events by ensuring high availability to the users, shareholders and customers.

According to Hiles (2003) in the event of a disaster the recovery of any organization is dependent on the successful development, adoption and implementation of a Business Continuity Plan (BCP). Accordingly it is akin to putting the cart before the horse by having a DR plan without BC plan as it is does not make sense to mitigate against a disaster without a plan. The key questions of concern here are: How should the

organization proceed after a disaster? How much down time can be tolerated after a disaster? What programs are in place to ensure that Business operations are affected to a minimal extent?

British Standards Institute (BSI) standard BS 25999-1:2006 defines business continuity management as process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response which safeguards the interests of its key stake holders, reputation, brand and value creating activities. This therefore means that BCM is inclusive of disaster recovery, business recovery, crisis management, incident management, emergency management, product recall, and contingency planning.

Blyth (2009) noted that as a component of the overarching Business Continuity Management Plan, the incident management plan (IMP) provides the vehicle by which employees can receive both training and instruction on how to respond to a crisis, regardless of their professional backgrounds or appointments within the company—supporting enterprise resilience from the bottom up. The IMP provides a mechanism for bringing confidence on how to respond to, and enable control of, a crisis. Psychologically, people perform better when they believe they have control over a situation, and the incident management plan offers a method by which companies can provide such confidence, guidance, and direction to managers and employees. The incident management plan forms a pragmatic component of an overall contingency planning and crisis management approach, offering education as well as realistic and user-friendly guidelines and simple procedures by which to support inexperienced first-line responders, as well as more experienced and competent incident management and crisis response teams.

1.1.4 Steps in Business Continuity Planning

Williamson (2002) found there are five main steps in the business continuity planning process. The process involves a five part process as follows: a) Initiation- Involves planning for the initial meeting with senior management. For this to be successful one

must know as much as possible about the issues associated with the development of disaster planning. To secure the senior management support necessary for success, you must present a well thought out approach and demonstrate management control of the proposed project; b) Business Impact Analysis- The data gathered is pivotal to identifying key business issues and justifying to executives the resources needed. The BIA determines the financial exposures and operational impacts resulting from a major disruption of services. It will provide your organization with the identity of its time-sensitive business operations and services, an analysis of the organization's financial exposures and operational impacts, the time-frames in which time-sensitive operations, processes and functions must resume as well as an estimate of the resources necessary for successful resumption, recovery and restoration.; c) Disaster Readiness Strategies- this involves defining and costing the business continuity alternatives, recommending disaster readiness strategies, preparing senior management reports and presentations as well as obtaining disaster readiness strategy approval; d) Develop and Implement the Plan- It should include step-by-step instructions on what to do, who should do it, and how. List each responsibility and write down the name of the person assigned to it. Also, do the reverse: For each person, list the responsibilities. Also make sure everyone in your company knows the BCP and hold mandatory training classes for each and every employee whether they are on the critical list or not; and e) Maintenance and Testing- finally run the test. If you make any major changes, run it again a few months later and test it on an annual basis.

1.1.5 Parastatals

According to a 2006 Handbook for Civil Service Staff induction, a Parastatal is a state corporations and agencies mainly established by a statute or an Act of Parliament in pursuance of Government policy. They are connected to the central Government by virtue of their functions and they work in close co-operation with appropriate Government departments. Parastatals are Quasi-Government agencies affiliated to Government operations. They are public enterprises.. Their legal status varies from being a part of government into stock companies with a state as a regular stockholder. In

Kenya, parastatals are classified into three categories namely class A, class B and class C parastatals. The categories are based on the revenue base, size and the ministry the parastatals falls under. Parastatals are further classifieds in terms of industries they belong to. The sectors include: Financial sector, commercial/manufacturing sector, regulatory sector, public universities, training and research, service corporations, regional development authorities, and finally tertiary education and training.

1.2 Problem Statement

In the past, many parastatals hardly defined disasters and those that did defined them as an act of nature e.g. a flood or fire that wipes out their ability to conduct business as usual. Today, with worldwide networks, 24/7 customer call centers and Web applications, a common electrical failure could spell disaster when communication is interrupted in the supply chain, real-time transactions are halted or networks are down.

The amount of critical information held by parastatals as a result of automation is very important for their efficient and effective service delivery. For this to happen without interruption there is the need to have disaster recovery mechanisms and business continuity plans to support business and ensure critical information is maintained without any loss. According to Juniper Networks (2009) a business continuity plan in Government is a need to ensure that essential functions can continue during and after a disaster. This includes the prevention of mission critical service interruptions, and the ability to re-establish full functionality as quickly as possible. In essence, the plan pays as much importance to the man power as the technology and the data to be recovered.

Strohl Systems, a Pennsylvania-based provider of business continuity planning software to corporations worldwide, annually surveys hundreds of businesses regarding their business continuity programs and in a survey conducted in April 2005, one out of every eight organizations in has experienced decreased insurance rates due to a comprehensive business continuity plan. Another conducted in May 2006 found that 38% had activated

there business continuity plans. The importance of business continuity, business continuity planning has not often been deemed a high priority. Instead, an alarmingly large number of companies have been "assuming" that their existing systems will be adequate for emergency situations. This lack of preparedness is unwise for all, and it is definitely not an option for government departments and agencies.

Disaster recovery and business continuity planning are relatively emerging concepts in Kenya. Locally, disaster recovery and business continuity planning are relatively emerging concepts in Kenya. Nyambura (2005) carried out a survey of ICT aspects of disaster recovery among companies quoted at the NSE as well as Muoki (2010) who carried out a research on business continuity planning for a global business operator in less developed economies, a case study of general motors East Africa. Though most organizations have known about the practices and or concepts very few organizations have gone the extra mile and implemented any of this more so in the public sector. It is only very recently that parastatals began realizing the need to protect the vast amounts of crucial information, maintain the integrity and accuracy of this information. Ensuring business continuity measures are in place in case of disasters is becoming critical to the success of many parastatals. It is in light of this that disaster recovery and business continuity has become relevant to many organizations both in the private and public sector.

This study therefore aimed to answer the following research questions what business continuity and disaster recovery measures have been put in place? What benefits have been derived from implementation of business continuity and disaster recovery measures? And finally What challenges have affected or hindered the implementation of disaster recovery and business continuity plans?

1.3 Research Objectives

The general objectives of this study were to assess the disaster recovery and business continuity plans of class-A parastatals in the various government ministries. Specifically the study intended:

1. To establish the extent to which class-A parastatals have implemented business continuity and disaster recovery mechanisms.
2. To determine the benefits that class-A parastatals have derived from implementation of business continuity and disaster recovery
3. To analyze the challenges experienced by Class A parastatals as they establish DR and BC plans.

1.4 Value of the study

This study is important for many reasons but primarily to managers the study would help ICT managers' of Parastatals in Kenya in understanding and appreciation of the need for business continuity and disaster recovery. Managers would also be made aware of the challenges that have been experienced in the adoption and implementation of business continuity and disaster recovery and this would help them make appropriate adjustments to counter these challenges and achieve optimal results. To regulators and policy makers, the study provided insights on the strategies that can enhance the ICT and Parastatals sectors' growth, and hence guide in regulation and policy formulation. This therefore helped policy makers in government among others with the development and review of existing policies to achieve synergy with the existing circumstance. To researchers and academicians, the study availed material for reference by future researchers and academicians on the same topic of business continuity and disaster recovery. In addition, the study also highlighted other topics of future research like cloud computing issues in disaster recovery and business continuity in Kenya.

CHAPTER 2: LITERATURE REVIEW

2.1 1ntroduction

Laye (2002) suggests that given today's pace of business, including government's business of providing services, and the expectations of your organization's customers (whether your organization calls them customers, clients, taxpayers or constituents), no manager or policy maker can afford to be regarded as so inept that he or she lacks foresight to make effective preparations, minimizing the impacts of dangerous events. In view of this, even parastatals have now recognized they need to plan for any eventual disruptions to business functions due to the nature of services the offer their clients or taxpayers. This has necessitated they need to invest in infrastructure (IT systems and services) to minimize the impacts of disasters and loss of any information. It is almost impossible to have disaster recovery and not have business continuity or vice versa because the two have been known to go hand in hand. The importance of the two is recognized in the importance mangers have attached to ensure that downtime in there organization are minimized to the bare minimum since it's impossible to eliminate downtimes completely.

Myers (1993) asks a fundamental question which comes first, the chicken or the egg? Which comes first in contingency planning? Recovering lost technology or keeping the business running? The business continuity plan should come first. In fact when data processing, plans to recover technology are developed before a business continuity plan, it normally results in an excessive amount of resources committed to redundant computer processing capability. Williams (2002) suggests that being prepared is crucial to protecting your organization in case of a systems disaster. Likewise, lack of planning is the same as planning to fail hence the need to have the business continuity plan before disaster recovery. The technology used in disaster recovery is born out of having a good plan in place hence emphasize is on having the plan before the technology.

2.2 Critical Elements of a Business Continuity Policy

According to Protiviti (2006), an independent risk consulting firm a growing number of firms organizations rely on a formal, documented business continuity policy to drive the business continuity program. Although the content and the format of the BC policies differ based on existing standards and the culture of the organization they recommend the following nine elements to drive the process towards an optimal level of maturity: First element is accountability which involves naming executives accountable for the BCM planning and the responsibility for resources and strategic decision making. This aids in knowing whom to contact, when and for what. The second element is roles and responsibilities which defines roles and responsibilities for all employees regarding planning and activities before, during and after a disaster. The third is analysis which establishes the need for and standards associated with risk assessment and business impact analysis which is the corner stone of the planning effort.

Fourth is legal, regulatory and contractual assessment which requires the participation of the legal department to ensure compliance of the law as well as customer contractual requirements impacting business continuity strategies. The other is business continuity execution which identifies specific actions necessary to develop optimal BC strategies that meet business requirements. The other is business continuity strategy and plan maintenance which specifies the standards regarding the review and maintenance of business continuity analysis, strategy and documentation. The seventh element is testing (exercising) which defines the test types, frequency of tests as well as objectives of the test. The eighth is training and awareness which sets the specifics on personnel training named in response and recovery plans as well as general awareness of employees affected by the BC strategies; and finally internal audit preparation emphasizing participation of internal audit in the planning process and/or the review of compliance with the requirements set forth in the BC policy.

2.3 Business Continuity Planning

A Business Continuity Plan (BCP) is the least expensive insurance any company can have especially for small companies, as it costs virtually nothing to produce. Unfortunately, many companies have never taken the time to develop such a plan. According to International Standards for Organizations (ISO) ICT Readiness for Business Continuity (IRBC) supports Business Continuity Management by ensuring that the ICT services are as resilient as appropriate and can be recovered to pre-determined levels within timescales required and agreed by the organization. ICT readiness is important for business continuity purposes because: a) ICT is prevalent and many organizations are highly dependent on ICT supporting critical business processes. This ideally implies that even in Kenyan parastatals today ICT has become a key driving force in the organizations. Most have realized that one of the growth strategies needed to enhance efficiency; b) ICT also supports incident, business continuity, disaster and emergency response, and related management processes. In essence recovery is usually pegged on the computerized recovery systems that the parastatal has in place since recovery lost documentation is practically impossible; c) Business continuity planning is incomplete without adequately considering and protecting ICT availability and continuity. ICT being the backbone of many parastatals, it therefore only makes sense to have BC plans that incorporate ICT as without IT then very little data and information will be recovered.

Snedakar (2007) suggests that continuous availability is a subset of business continuity. It's also known as a zero-downtime requirement, and is extremely expensive to plan and implement. For some companies, it may be well worth the investment because the cost of downtime outweighs the cost of implementing continuous availability measures. While as the Kenyan situation may vary from one Parastatal to another it more or less goes to show that disaster recovery and business continuity plans and management are key to the continued operation of any organization especially where data is very vital e.g. Customer Records at National Hospital Insurance Fund and National Social Security Fund, tax records of tax payers at Kenya Revenue Authority or ullage allocation details at Kenya Pipeline Company storage tanks. All this parastatals, listed as class A parastatals by the

government, require disaster recovery and business continuity plans by the nature of transactions they have and sensitivity of the data they store.

Myers (1993) argues that although it is important to recognize the specific types of disasters that might occur to a given company or business environment, it is equally important to understand what the impact might be under worst case conditions. The process of uncovering these exposures is not unlike a long range business strategic planning process. In essence this lays emphasize on the need to have someone skilled in conducting a business impact analysis in conjunction with senior managers to visualize and anticipate problem areas, to document the exposure, and to formulate guidelines that will either prevent or minimize the impact of a particular type of disaster. Therefore putting business continuity plans into practice in your organization now can prepare your business for most any potential disaster, help ensure that you will be able to maintain continuity of your business practices, and reduce or even possibly remove the effect such calamities could have on your organization.

2.4 Steps in Business Continuity Planning

Williamson (2002) noted that creating and maintaining a workable business continuity plan (BCP) is an essential factor in ensuring your organization's continued survival and prosperity. Although planning methodologies may vary among organizations, there are standards common to all. The following are the five key steps in BC Planning:

2.4.1 Initiation

This is the initial meeting with senior management in the organization for without their support little would be achieved in this regard. Some of the key steps in planning for this meeting include: Reviewing the organization to determine what resources are appropriate to be assigned to the project team. This involves reviewing any existing enterprise-wide disaster plans, policies, strategies and procedures relative to emergency response or continuity of operations. The other is review of any continuity plans that are in place

within the organization and assess if they are effective models for the project. The third is research local events in the recent past such as fires, severe weather, major equipment failures, etc. that had or could have had a negative effect on the organization. The fourth is review any pertinent laws and regulations that may affect or hinder project. The other is preparation of a project introduction Memo for senior management's signature to communicate to the organization at large the need for BCP and the program's goals. Another step is preparation to discuss project funding by ensure that management realizes that business continuity planning is an ongoing budget item, not a one-time project.

The seventh is research and recommend any necessary training for yourself or other members of the proposed project team. Another is to ensure access to personal computers for all team leaders. If you've purchased and are using a LAN version of your BCP software, make sure that a server has sufficient space and capacity to run the program and also budget for any required computers. The ninth step is drafting the project schedule. This can be a draft or tentative version but should contain the important tasks, timing and resources required to accomplish your objectives. Start with the basics and add detail as necessary. A project management software package might be a worthwhile investment if your Coordinator is comfortable with its functions; and lastly invite a management representative to the kick-off meeting from every department or section that will be helpful in presenting a more thorough understanding of the project.

2.4.2 Business Impact Analysis (BIA)

Involves identifying the impacts that result from disruptions that can affect the organization and the techniques that can be used to quantify and qualify such impacts. Okolita (2009) says that this is the process that will determine what needs to be recovered and how quickly. It is one of the most difficult tasks to perform and one of the most critical to get right. The more time you have to bring a business function back in service following a disaster, the more your recovery options increase. The business impact analysis is invaluable for identifying what is at stake following a disaster and for justifying spending on protection and recovery capability. Nobody but you will mind

your own business. Since the business impact analysis is among the first steps in the business continuity planning process it is important to draft a proper questionnaire that will aid in gathering all the relevant areas of potential loss and undesirable effect such as loss of customer confidence, reputation damage, and regulatory effects.

Hiles (2003) states that a Business Impact Analysis (BIA) is the identification of the effect on the organization of the risk to it should they occur. The business impact analysis process achieves a number of objectives, namely: a) Identify the financial and non-financial costs; b) Establishing the time window in which recovery has to take place; c) Identifying vital materials and records necessary for recovery or continuance; d) Making a preliminary assessment of resources required for recovery or continuance; and e) Providing input to the Risk assessment on business risks that may not otherwise be identified.

The purpose of a risk assessment is to identify the internal and external threats that could cause a business interruption and assess their probability and impact of a variety of specific threats. The risk assessment studies all aspects of threats including physical, environmental, administrative, and technical measures. It provides a complete identification, sourcing, and evaluation of the risk at which an organization operates and puts the vulnerabilities in perspective for the business. It may be possible to implement measures to reduce the likelihood or mitigate the impact of these threats by prioritization on the most urgent business functions identified during the business impact analysis. A function may be considered critical if the implications for stakeholders or damage to the organization are regarded as unacceptable. A scenario in which KRA lost data pertaining to tax defaulters would be a serious and major loss which in this day and age cannot be tolerated.

Perceptions of the acceptability of disruption may be modified by the cost of establishing and maintaining appropriate business or technical recovery solutions. A function may also be considered critical if dictated by law. For each critical (in scope) function, two values are then assigned: a) Recovery Point Objective (RPO) - the acceptable latency of

data that will be recovered. With the advent of real time processing capabilities and the subsequent technological advances the latency of the recovered data has narrowed very much; and b) Recovery Time Objective (RTO) - the acceptable amount of time to restore the function. Disaster recovery mechanisms in place today have significantly reduced the restore time to almost a bear minimum, if at all any.

Okolita (2009) notes that all business functions and the technology that supports them need to be classified based on their recovery priority. Recovery time frames for business operations are driven by the consequences of not performing the functions. The consequences may be the result of business lost during the down period: contractual commitments not met and resulting in fines or lawsuits, lost goodwill with customers, etc. Impacts generally fall into one or more of these categories: financial, regulatory, or customer retention. Williamson (2002) found that every major business operation should be evaluated using the BIA approach. Each line manager must be aware of the length of time that a particular service, business operation or application system may not be available, and devise interim procedures to ensure the continuity of the most time-sensitive activities. The minimal outage time allowable for each business operation must be documented and endorsed by senior management. Senior management may be called upon to refine business time-sensitivity definitions, adjust resumption priority sequences or allocate additional resources and funding where resumption capacity becomes an issue. The project team should use this information to support the organization's strategies and any necessary investments in backup alternatives.

2.4.2.1 Business Impact Assessment Interview

Every major business operation should be evaluated using the business impact assessment approach. Each line manager must be aware of the length of time that a particular service, business operation or application system may not be available, and devise interim procedures to ensure the continuity of the most time-sensitive activities. According to Williamson (2002) the project team should be able to gather the following information from the business during the BIA: First is the financial impact to the

organization resulting from each business operation's inability to conduct operations for a prolonged period of time- this will basically assess how much revenue the business is likely to lose during downtime over a period of time. The second is operational impacts relating to each business operation-this will address what installation, systems, processes and functions are affected by any downtime. The third is extraordinary expenses involved in continuing operations after a disruption-this will address what expenses on mission critical systems or functions will be incurred during the duration of a downtime. The fourth is the current state of preparedness to resume business operations which reviews the organizations ability to continue normal operations in the event of downtime. The fifth is the technology requirements for resumption and recovery which addresses issues of hardware, software and offsite location necessary for resumption and recovery in the event of downtime. The sixth is other special resumption and recovery resources- reviews what other resources would be required in resumption. This might include employees, vendors and contractors. And lastly is Information Systems support for resumption of time-sensitive operations.

2.4.3 Disaster Readiness Strategy

Williamson (2002) identified the following as the strategies to include:

Define and Cost Business Continuity Alternatives- Using the information from the BIA, the project team should evaluate the alternative strategies that are available to the organization, narrow the list of alternatives to the two or three most plausible, and develop budgetary costs for each strategy. The resumption timeframes will play a significant role in determining which components may require prepositioning; Recommend Disaster Readiness Strategy- Based on the needs of the business and your evaluation of alternatives, the project team should develop recommendations on which strategies to fund for implementation;

Prepare Senior Management Report and Presentation- Prepare a formal report and presentation on the findings of the BIA, the strategy alternatives that were developed and

investigated, and the project team's recommendation; and Obtain Disaster Readiness Strategy Approval- Obtain approval from senior management to proceed with the project. Ensure that they understand and approve the funding required to continue the project and to implement the selected strategies.

2.4.4 Develop Disaster Recovery and Business Continuity Plan

Williamson, J (2002) suggests that creating and maintaining a workable business continuity plan (BCP) is an essential factor in ensuring your organization's continued survival and prosperity. Although planning methodologies may vary among organizations, there are standards common to all. Likewise in Kenya, parastatals need to critically plan as a mitigation strategy towards minimizing downtimes when disasters occur. This they cannot do in isolation as standards have already been established on how to best implement BC plans some of which can be customized for the particular industry. Wold (1997) asserts that the primary objective of disaster recovery planning is to protect the organization in the event that all or parts of its operations and/or computer services are rendered unusable. Preparedness is the key. The planning process should minimize the disruption of operations and ensure some level of organizational stability and an orderly recovery after a disaster.

Therefore the goals of Business Recovery Plan should be to: a) Identify weaknesses and implement a disaster prevention program; b) Minimize the duration of a serious disruption to business operations; c) Facilitate effective coordination of recovery task; and d) Reduce the recovery effort. This is a guide to the stages of a vulnerability assessment that outlines the vulnerabilities the organizations is exposed to. This is followed by a business impact assessment where the criticality of the vulnerabilities is assessed in reference to their impact to the running of the business. After successful completion of these tasks a plan of recovery can then be made. Regular review of this plan is necessary to ensure that it is a working policy.

The successful and cost effective completion of such a project requires the close cooperation of management from all areas of Information Systems.

Kurtz (2008) also noted that the steps below are very important when developing a business continuity plan. They include planning for a wide range of possible scenarios as downtime, whether it is a result of a hurricane, fire, power outage, hardware failure, or human error, affects your IT infrastructure and ultimately your productivity and bottom line. When developing a disaster recovery strategy, your company should consider various possible disaster scenarios and plan accordingly. Parastatals in Kenya would likely consider power outage, sabotage especially when trying to hide corruption related information, flash floods amongst others; Secondly, understand your time and data requirements- Determine how much time your company can afford to be down as well as how much data you can afford to lose. Armed with this knowledge, a parastatal can balance recovery requirements and risk tolerance, and budget how much you are willing to spend on a disaster recovery strategy; Third, look to keep your people, systems, and information connected- Your business continuity strategy must encompass information, systems, people, and processes, as well as the complex interdependencies among them. If your workforce cannot connect to systems and data, there is no business; fourth is to investigate advanced technologies- Disaster recovery technologies have changed considerably in recent years, and solutions that were once only common in large enterprises, such as replication, vaulting, and virtualization, are now becoming more accessible in Kenya. These technologies would greatly assist parastatals in achieving an even greater precision in recovery time frames and data points; and finally plan and test- Planning involves much more than just backing up your data. Many companies think they have an effective disaster recovery plan, but unless it is tested, it is only a plan on paper and not in reality. It is essential for your company to develop and test your plan so the first time it is executed is not during an emergency. Industry research firm Yankee Group recommends running a disaster recovery test every quarter to help ensure your protection mechanisms will actually protect you when you need them most.

2.4.5 Maintenance and Testing

The steps here include:

The first is to establish a plan exercise program- Develop and conduct plan exercises. Exercises will grow in complexity over time. Include announced and unannounced events. Document your objectives for each exercise. Individual objectives should include responsibility assignments and measurement criteria. Evaluate the results of each exercise against pre-stated measurement criteria and document results along with proposed plan enhancements. Secondly, establish training requirements bearing in mind that team training will vary from plan to plan and by the category of team (e.g., operations, support and technology). The complexity of the environment and the time-sensitivity of the functions will guide the project team in the development of training. Training materials should cover all Steps of disaster readiness planning. Third is to sample emergency response exercises where emergency response exercises should be ongoing, quarterly events using alternate scenarios and should involve every organization within a particular facility that may be affected by a system disaster.

2.5 Benefits of Implementing Business Continuity

Business continuity and disaster recovery plans are essential components of overall business and IT planning. Since disasters do happen, it's critical to have business continuity and disaster recovery plans in place before the need arises. There are very many reasons why Government, government agencies and business implement business continuity. According to Belshaw (2008) the following are some of the top 10 reasons that business implement business continuity plans: a) survival: For parastatals offering critical services to the masses, a business continuity plan can make a huge difference in service delivery; b) revealing inefficiency: Enables organizations to determine what products or services are critical as well as the resources required to keep them running; c) market edge: For parastatals that have competitors in the market e.g. East African Portland Cement, the need to maintain and grow their market share is reason enough to have solid business continuity plans; d) boosting staff morale: Employees are loyal when

they know the organization has put in place measures to safeguard their livelihoods; e) reduce on insurance premiums: A parastatal can have its insurer reduce its premiums if it demonstrates commitment to managing risks; f) legal compliance: The demand for business continuity plans is now trickling down from big business to their smaller suppliers. The Central Bank of Kenya has recently established business continuity regulations for banks which they must be adhered to; g) better communication: being able to give the right person (who can fix the problem), the right info, at the right time is a critical reason to have BC plans in-case of a disaster as it addresses who does what, when, where and using what resources; h) increased value: A business that will cope with whatever is thrown at it is a more valuable and reliable investment than others; i) negotiating tool: Understanding the principles of business continuity means you can spot weaknesses in other businesses. This can thus be used as a bargaining tool e.g. with banks; and j) peace of mind: While other parastatals heads and business people lie awake at night, you can rest easy knowing your business continuity plan is ready, should the worst happen.

2.6 Top Mistakes Companies make in Disaster recovery

Hager (2010) noted the following pitfalls:

Inadequate planning: the first step here is to identify all critical systems, and having detailed plans to recover them to the current day. More often than not most people think they know what they have on their networks, but they really don't know how many servers they have, or how they're configured, or what applications reside on them-what services were running, what version of software or operating systems they were using;

Failure to bring the business into the planning and testing of your recovery efforts: The major problem arises when IT department isolates other departments and makes the project an IT project. In essence the IT component of the business continuity plan is largely the disaster recovery part while as BCP encompasses the organization as a whole.

Failure to gain support from senior-level managers: The largest problems here are not demonstrating the level of effort required for full recovery, not conducting a business impact analysis and addressing all gaps in your recovery model, not building adequate recovery plans that outline your recovery time objective, critical systems and applications, vital documents needed by the business, and business functions by building plans for operational activities to be continued after a disaster, and not having proper funding that will allow for a minimum of semiannual testing.

Disaster recovery planning is a sensitive topic amongst most IT managers. Due to the increased numbers of disasters whether through terrorist attacks or natural calamities, more and more boards are focusing on this issue. The events of 7 August 1998 are still fresh in our minds. Many organizations now realize that indeed Kenya lies within the global arena and as such is affected by incidences like terrorist threats. With that realization, many organizations have DR and BC plans that encompass this kind of scenarios. The IT staff in most companies is very capable of recovering from many types of outages. After all, these are the very people who designed and built the system in the first place. They know where every wire in the organization runs and have more committed to memory about the infrastructure than most of us could learn in a decade. Therein lies the problem. What if the very same people who are supposed to perform the recovery are themselves unavailable? A good DRP should be well known by all as any co-worker can be called upon to execute it in the absence of those who are normally responsible for it. A good business continuity plan requires the adoption and support of disciplines such as: a) Backup Management; b) Storage Management; c) Configuration Management; and d) Security Management. Redundant computer systems have become extremely popular over the past several years as business continuity solutions, particularly for organizations that require uninterrupted processing for their business systems. In theory, should a failure occur, the duplicate systems would immediately assume processing responsibility with little or no disruption. Obviously, to make this work, it's not just the hardware that's duplicated, but also the information stored within the system.

2.7 Five Steps to Evaluating Business Continuity Services

Collet (2007) noted that companies are stepping up their use of hosted business continuity (BC) and availability services—not just for those acts of nature, but also for everyday occurrences that might interfere with stringent uptime requirements. The market size for capital expenditures on in-house servers, storage and internal staff used for business continuity and disaster recovery is harder to quantity. Very often, that server and storage infrastructure can be brought in to support other applications and initiatives. Although it still needs to be backed up and may have to be managed, restored and brought back to production, it is not always counted in the disaster recovery budget. Some points to consider when evaluating business continuity and availability services and software include:

Weigh the benefits of specialized business continuity planning software: Business continuity planning software can help large companies formalize the BC framework and continually update the plan. "Of companies that actually have plans, 50 per cent use software and 50 per cent use informal software" such as Excel spreadsheets. The software plays a very important role in updating plans, collaborating, invoking and tracking that all the tasks are being executed;

Consider the major business continuity/availability service providers and some niche players: Hosted business continuity/availability providers typically provide cold sites (data center space to house your own equipment and backup tapes), warm sites and hot sites (an operationally ready data center), as well as data archival, restoration capabilities, managed services;

*Let recovery requirements dictate the level of dedicated BC services***:** Subscribing to a data recovery service that you can trigger when a disaster strikes is fine if data can be restored in two to four days. But increasingly, as businesses require 24/7/365 availability, more dedicated data recovery services are required. If you have to recover within 24 hours, that requires some form of dedicated infrastructure in terms of remote SAN

[storage area network]. If you're using asynchronous replication or data mirroring, you've got to have fixed assets that are using the data backup;

Don't forget emergency notification systems: One of the ways companies use notification systems is by having an escalation matrix which is basically a matrix showing the elevation levels of a problem, who is responsible at each level, the resources available to the personnel as well as the response time. Emergency notification systems can use many different means of communication—phone calls, text messages, e-mail—to contact employees, vendors or other critical personnel. Companies should also consider having an automatic phone forwarding system through the phone company. That way, clients whose only contact is an office phone number can be rerouted to an employee's cell or home phone; and

Use caution when outsourcing business continuity functions overseas: Because of terrorism and natural disasters typically not seen in Kenya such as the bomb blast in 1998, companies should take caution when outsourcing backup, recovery and business continuity operations offshore. In many organizations the issue of outsourcing sensitive company information is usually a policy level guided by the board. In parastatals, that decision would be guided by the current government policy regarding such issues. However it is important to consider the background of the company that you will be outsourcing too, the legal (or otherwise) limitations, freedoms and protection the data you have is subjected to, the government policy regarding data handling as well as the economic and political stability of the country.

2.8 Problems in Implementing Business Continuity and Disaster Recovery in Government/Parastatals

According to Jupiter network Inc (2009) today more than ever, government agencies and enterprise businesses of all sizes are dependent on a variety of applications and resources to access, store, and process critical information for their business functions. The

following were identified as challenges in implementing business continuity in third world countries by Singh (2009):

The first is project sponsor is changed at crucial juncture – Government officials are transferred on regular basis; it might happen that newly transferred project sponsor is not interested in the new BC and DR project. The second challenge is change of government which case for parastatals a change of government can signal the end of a project whether or not it was completed. It can also signal change of policy thereby derailing the business continuity project. Sometimes it is a difficult and tough time in managing new set of customer stakeholders. Thirdly is the lack of interest of by the project sponsor which might result in issues such as whether to outsource or build an in-house DR site or merely finding no need to support the project as a priority. Another challenge is the huge difference in work culture. In some instances email communication is not very frequent in most of the government offices of developing countries while lots of physical movement is required to keep project stakeholders in synch with the progress of project work. In such a scenario as the latter the need for BC might not be as important as where email communication is very important.

Another challenge is where only hardware is considered for the project. Parastatal heads sometimes do not understand the software needs of IT projects. They assume hardware is the only important item required for the project whereas the software aspects of a DR and BC project might be quite expensive and important. The sixth challenge is the conflicts of interest in influential project stakeholders. In DR and BCP projects there are usually three to four departments involved and it constantly creates incompatible situations where project decision making stakeholders are not in synch with each other. The project can turn out to be an ego issue for them. The seventh is business reengineering challenges whereby most of the countries have their work processes set according to policies last reviewed years ago thereby making it tough to induce BCP in existing work processes where even convincing the critical users is very tedious job. There are statutory issues involved as well to disallow any change in the existing processes but important for new system. The eighth challenge is identification of right stakeholders which involves

identifying all the important stakeholders as project managers are normally unaware of the roles and responsibility of different departments. Another challenge is dishonesty by project vendors responsible for creating new products adopt side ways to keep project going. These unavoidable practices are an integral part of government projects in developing countries; and finally delays in payments due to beauracracies thereby making it very tedious job for account managers to get the regular payment invoices cleared and to receive timely payments in parastatals.

2.9 Best Practices

According to Janco Associates, Inc which focuses on Business Continuity and Disaster Recovery, the following are best practices that should be incorporated in implementing business continuity: a) focus on operations - people and process that drive the enterprise are the primary issues that DRP and BCP are controllable; b) train everyone on how to execute the DRP and BCP - People are the front line when it comes to supporting the enterprise and any DR and BC Plans; c) have a clear definition for declaring when a disaster or business interruption occurs that will set the DRP and BCP process into motion; d) integrate DRP and BCP with change management; e) focus on addressing issues before they impact the enterprise; f) validate that all technology is properly installed and configured right from the start; and g) monitor the processes and people to know what critical processes are being omitted or not being implemented accordingly.

2.10 Business Continuity and Disaster Recovery Conceptual Framework

Wilder (2008) noted that the Information Technology Infrastructure Library (ITIL) is an Information Technology (IT) management framework that provides practices for Information Technology Services Management (ITSM), IT development and IT operations. ITIL gives detailed descriptions of a number of important IT practices and provides comprehensive checklists, tasks and procedures that any IT organization can tailor to its needs. The ITIL-ISO 2000 model defines IT Service Continuity Management levels to ensure management controls and processes are in place to meet the service level

requirements. The new ITIL v3 model has been introduced and provides a more holistic perspective on the full life cycle of services, covering the entire IT organisation and all supporting components needed to deliver services to the customer. ITIL is based on 5 core lifecycle titles include Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement

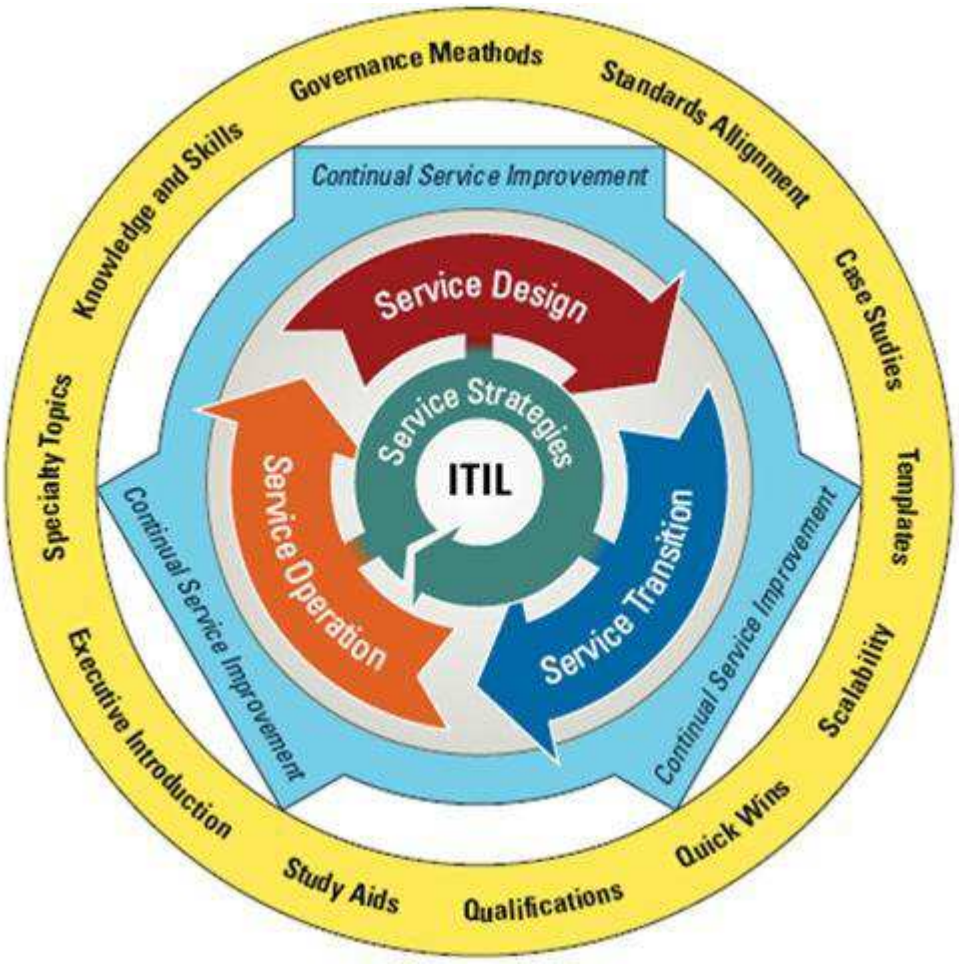


Figure 1: ITIL v3 Model

Service Strategy focuses on helping IT organisations improve and develop over the long haul. The key indicators include service value definition, business-case development, service assets, market analysis, and service provider types. Service design provides guidance on the design of IT services, processes, and other aspects of the service management effort. Significantly, design within ITIL is understood to encompass all

elements relevant to technology service delivery, including business continuity and disaster recovery, rather than focusing solely on design of the technology itself. Service transition relates to the delivery of services required by a business into live/operational use, and often encompasses the IT side of things as opposed to the business. It also focuses on issues of change management due to impending changes in the business environment. Service operation focuses on delivery of agreed levels of services both to end-users and the customers. It is the actual point in time where services and related value additions are derived by the business. It also involves monitoring the services and ensuring reliability. Finally, continual service improvement involves reassessing IT services to changing business needs to avoid stagnation. In this case it's important that business needs are identified early enough for improvements as they support the business to achieve organization's growth strategies.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

The purpose of this study was to identify business continuity and disaster recovery measures that have been implemented in class-A parastatals, the benefits derived from this and the challenges faced during implementation strategy implementation and finally to give recommendations. This chapter provided a discussion of the research methodology that was used in this study. It discussed the research design especially with respect to the choice of the design. It also discussed the population of study, sample and sampling techniques, data collection methods as well as data analysis and data presentation methods to be employed in the study.

3.2 Research Design

Research design refers to the procedures to be employed to achieve the objectives of the research. Through a research design the researcher conceptualized an operational plan to undertake the various procedures and tasks required to complete the study (Kumar, 2005). The research design employed in this study is descriptive in nature. Through the use of surveys the study will be guided by three independent variables; what BC and DR plans are in place, the benefits derived from the BC and DR plans, and determining the challenges encountered in implementing BC and DR plans. The study used a descriptive design because it enables the researcher to collect in depth information about the population being studied. The descriptive design gave proper and brief recommendations to the management of the various parastatals as well as other relevant government bodies and policy formulation organs.

3.3 The Population

A Mugenda and Mugenda, (2003) defined target population as the population to which the researcher wants to generalize the results of the study as was the case in this research.

Parastatals in Kenya are categorized in classes namely Class A, B and C. The study focused on Class A as they represent huge government corporations both in-terms of strategic importance, revenue and employees. The population consisted of the 18 parastatals as is in the attached appendix. The questionnaire targeted at least 3 senior and middle-level management employees making it an intended number of 54 recipients. The target population of senior management in many organizations mainly concentrated in formulating of strategies and crafting of the strategic plan for the company whereas the middle and lower level staff mainly deal with the implementations of the strategies that have been developed. In this regard senor level managers would give guidance eon the policy of the parastatals in DR and BC plans while middle level management would be involved in implementation.

3.4 Data Collection

The study primarily used data collected from questionnaires with the aim of ensuring that the respondents answer to the most comfortable of methods to them. The questionnaire was broken down into 4 sections namely section A with the respondent profile, section B with targeting the implementation process as a whole, section C the benefits derived from having DR and BC Plans and the fourth section D which focused on the challenges or problems encountered during the implementation.

3.5 Data Analysis

The data collected from this study was presented through the use of summarized percentages, proportions and tabulations and other data presentation tools in all the sections of the questionnaires. The analysis employed various analysis methods amongst them Statistical Package for Social Scientists (SPSS) and Microsoft Excel Spreadsheet

CHAPTER FOUR

DATA ANALYSIS AND INTERPRETATION

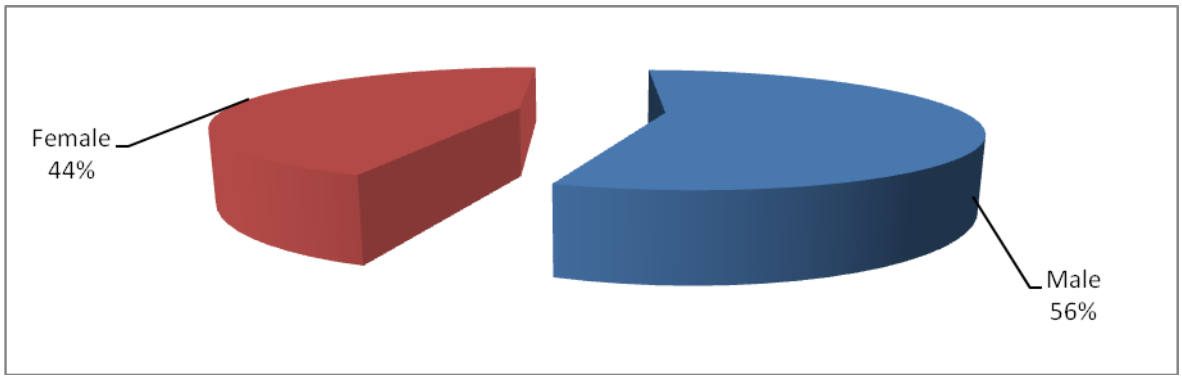
4.1 Introduction

This chapter presents analysis and findings of the study as set out in the research methodology. The study findings are presented on the disaster recovery and business continuity plans of class-A parastatals in the various government ministries. The data was gathered exclusively from the questionnaire as the research instrument. The questionnaire was designed in line with the objectives of the study.

4.1.1 Response Rate

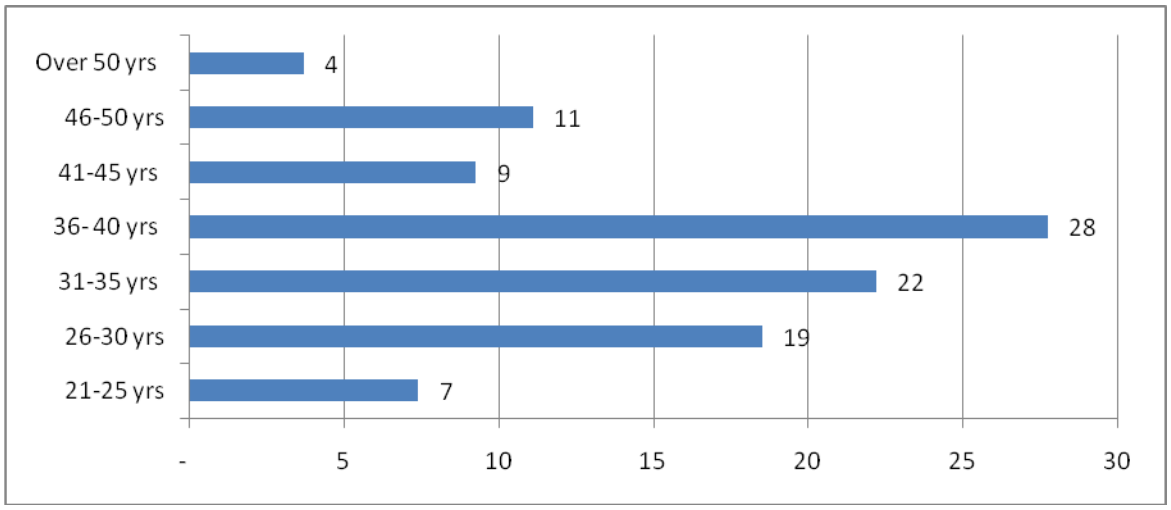
The study targeted 54 respondents in collecting data with regard to disaster recovery and business continuity plans of class-A parastatals in the various government ministries. From the study, 54 out of the 54 sample respondents filled-in and returned the questionnaires making a response rate of 100%. This reasonable response rate was made a reality after the researcher made personal calls and visits to remind the respondent to fill-in and return the questionnaires.

Figure 4. 1: Gender of the respondents



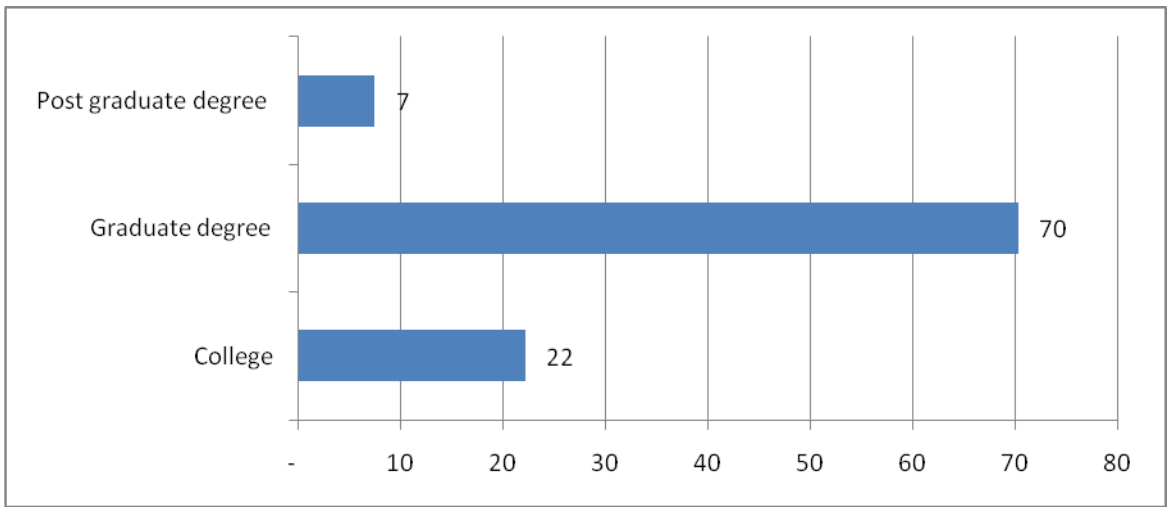
The study sought to find out the gender of the respondents. From the findings, 56% of the respondents were male while 44% of the respondents were female.

Figure 4. 2: Age of the respondents



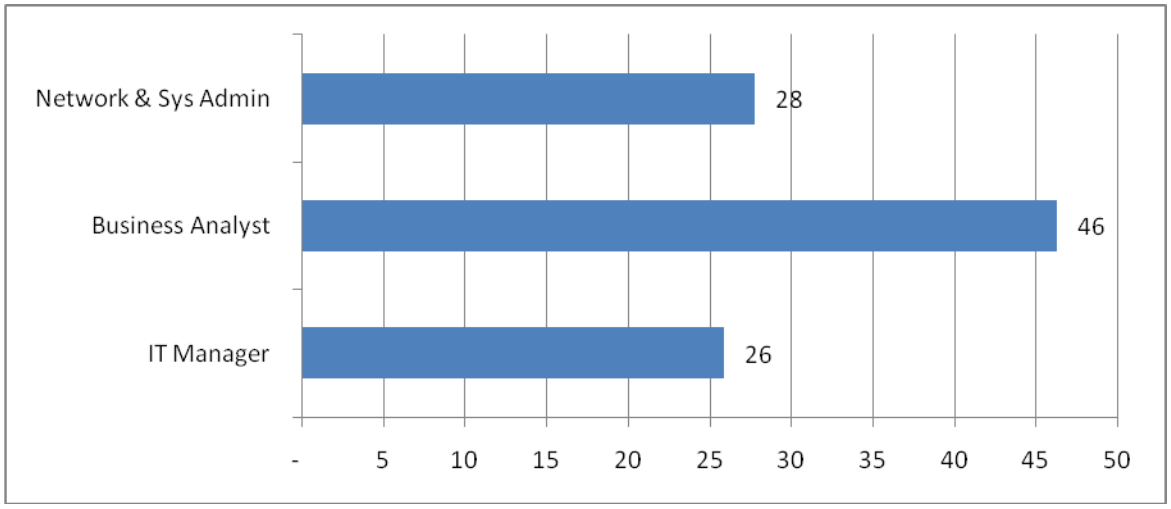
The study sought to find out the age of the respondents. From the findings, 28% of the respondents were aged 36-40 years, 22% of the respondents were aged 31-35 years, 19% of the respondents were aged 26-30 years, 11% of the respondents were aged 46-50 years, 9% of the respondents were aged 41-45 years, 7% of the respondents were aged 21-25 years and 4% of the respondents were aged over 50 years.

Figure 4. 3: Level of education of the respondents



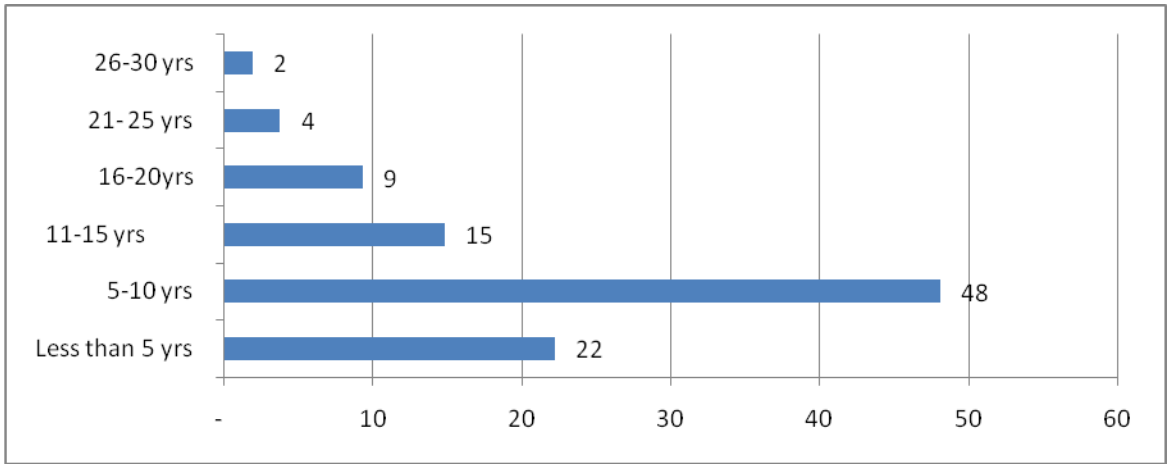
The study sought to find out the level of education of the respondents. According to the findings, 70% of the respondents had degree, 22% of the respondents had reached college and 7% of the respondents had post graduate degree.

Figure 4. 4: Designation of the respondents



The study sought to find out the designation of the respondents. According to the findings, 70% of the respondents were business analysts, 28% of the respondents were network and system administrators, 70% of the respondents were IT managers.

Figure 4. 5: Period the respondents had worked in the organization



The study sought to find out the period the respondents had worked in the organization. According to the findings, 48% of the respondents had worked for 5-10 years, 22% of the

respondents had worked for less than 5 years, 15% of the respondents had worked for 11-15 years, 9% of the respondents had worked for 16-20 years, 4% of the respondents had worked for 21-25 years and 2% of the respondents had worked for 26-30 years.

4.2 Pre Planning

Table 4. 1: Extent that the steps undertaken during the pre-planning phase

	No Extent at all	Small Extent	Moderate Extent	Large Extent	Very Large Extent	Mean	Stdev
Industry standard disaster recovery (DR) methodology	2	29	44	10	15	3.07	0.2
Perform a Business Impact Assessment (BIA) to prioritize your business processes	5	18	26	33	18	3.41	0.3
Consult business process owners during the BIA	7	21	21	30	22	3.42	0.5
Perform a risk management review to identify and correct obvious weaknesses	3	11	44	22	19	3.4	0.4
Preparation of a recovery options list that itemizes recovery options by business process	17	43	23	11	5	2.41	0.2

The study sought to find out the extent that certain steps were undertaken during the pre-planning phase of BCP and DR planning. According to the findings, the step that most respondents confirmed to have undertaken with by the majority was consulting business process owners during the BIA as shown by a mean of 3.42. The importance of this step is emphasized by the findings confirm what Chow (2007) that the purpose of a risk assessment is to identify the threats that could cause a business interruption and assess their probability and impact of specific threats. The other steps undertaken during the pre-planning phase were performing a risk management review to identify and correct obvious weaknesses to a large extent as well shown by a mean of 3.4 and adopting an industry standard disaster recovery (DR) methodology to a moderate extent as shown by a mean of 3.07. The other steps undertaken during the pre-planning phase were perform a Business Impact Assessment (BIA) to prioritize your business processes to a moderate

extent as shown by a mean of 2.59, and the steps undertaken during the pre-planning phase were preparation of a recovery options list that itemizes recovery options by business process to a small extent as shown by a mean of 2.41.

4.3 Plan Development

Table 4. 2: Extent to which the following steps were taken when developing the organization DR and BC plan

	No Extent at all	Small Extent	Moderate Extent	Large Extent	Very Large Extent	Mean	Stdev
Develop a disaster organization chart that defines recovery teams	12	15	22	33	18	3.3	0.8
Define a call tree for notifying your staff when a disaster is declared	2	5	38	37	16	3.54	0.2
Consideration been given to developing the BC plan around a worst case scenario	15	27	23	17	14	2.76	0.3
Measures to manage contingency processes while your IT systems are being recovered	8	8	28	28	25	3.45	0.1
Understand the company time and data requirements (e.g. how much downtime can the company afford)	20	35	25	14	5	2.46	0.2
Appoint a public relations team to address external inquiries	71	18	8	2	1	1.44	0.2
Develop a key vendors contact list	18	15	23	29	10	2.83	0.3
Vendors' approval for their inclusion in your plan (e.g., will they be available, under contract, etc.)	27	38	19	14	2	2.26	0.7
Inventory of assets needed for offsite recovery (example: backup tapes, operating system software etc.)	5	12	22	38	23	3.62	0.8
Document emergency response procedures to occur during and after an emergency	2	5	16	37	38	3.98	0.2
Formal system backup policy and schedule	2	10	15	29	44	4.03	0.4
Designate a location of backup tapes	1	5	14	49	30	3.99	0.7

List of detailed tasks needed for offsite recovery	2	5	38	37	16	3.54	0.3
Investigate new advanced technologies that can reduce downtime	12	13	22	33	20	3.36	0.3

The study sought to find out the extent in which various steps were under taken when developing the organization DR and BC plan. From the findings, developing the organization formal system backup policy and schedule was considered to have been undertaken by a majority to a large extent as shown by a mean of 4.03, while designation of a location for backup tapes was also undertaken by a large number and to a large extent as shown by a mean of 3.99. Likewise documenting an emergency response procedures to occur during and after an emergency was undertaken to a large extent as shown by a mean of 3.98, with the step inventorying of assets needed for offsite recovery (example: backup tapes, operating system software etc.) also undertaken to a large extent as shown by a mean of 3.62. Most respondents also undertook listing detailed tasks needed for offsite recovery as shown by a mean of 3.54 as well as defining a call tree for notifying your staff when a disaster is declared as shown by a mean of 3.54. Another step taken to a moderate extent when developing the organization BC and DR plan was measures to manage contingency processes while the IT systems are being recovered as shown by a mean of 3.45, as well as investigating new advanced technologies that can reduce downtime to a moderate extent as shown by a mean of 3.36. The other steps included developing a disaster organization chart that defines recovery teams indicated by a moderate extent with a mean of 3.3, developing a key vendors contact list to a moderate extent as shown by a mean of 2.83, consideration given to developing the BC plan around a worst case scenario to a moderate extent as shown by a mean of 2.76, understanding the company time and data requirements (e.g. how much downtime can the company afford) to a small extent as shown by a mean of 2.46, obtaining vendors' approval for their inclusion in the plan (e.g., will they be available, under contract, etc.) to a small extent as shown by a mean of 2.26, and lastly the least undertaken step undertaken by respondents when developing the BC and DR plan was appointing a public relations team to address external inquiries as is indicated by a mean of 1.44.

4.4 Plan Testing

Table 4. 3: Extent that test plans were used in the DR and BC Plan

	No Extent at all	Small Extent	Moderate Extent	Large Extent	Very Large Extent	Mean	Stdev
Development of a test plan	2	10	21	33	33	3.82	0.8
Segmentation of the overall plan into sections that are easily tested	22	30	33	12	1	2.34	0.2
Frequently scheduled tests	2	5	16	37	38	3.98	0.3
Use of incidents as a form of testing	2	20	44	22	10	3.12	0.1
Establishment of testing success indicators in the test plan	5	11	21	48	14	3.52	0.2
Total time for execution of recovery tasks as a success indicator	7	21	21	30	22	3.42	0.2
Testing of remote office connectivity as a success indicator	5	11	21	48	14	3.52	0.3
Testing of restored systems as a success indicator	7	21	21	30	22	3.42	0.1
Formal process to certify the success of your testing e.g. Test results documentation	3	11	19	22	44	3.9	0.2
Independent observer to validate the test results	18	40	12	18	13	2.71	0.3

The study sought to find out the extent that various aspects of a test plan were used in the DR and BC Plan. According to the findings, frequently scheduled tests was done in the DR and BC Plan to a large extent as shown by a mean of 3.98, closely followed by formal process to certify the success of your testing e.g. Test results documentation done by a majority of respondents to a large extent as shown by a mean of 3.9. Another key step undertaken was development of a test plan by a majority of respondents to a large extent as shown by a mean of 3.82, followed by establishment of testing success indicators in the test plan to a large extent as shown by a mean of 3.52. Testing of remote office connectivity as a success indicator was used in the DR and BC Plan to a large extent as shown by a mean of 3.52, total time for execution of recovery tasks as a success

indicator were used in the DR and BC Plan to a large extent as shown by a mean of 3.52, testing of restored systems as a success indicator were used in the DR and BC Plan to a moderate extent as shown by a mean of 3.42, use of incidents as a form of testing were used in the DR and BC Plan to a moderate extent as shown by a mean of 3.12. Lastly the steps least undertaken in the test plan while implementing a BC and DR plan were having an independent observer to validate the test results and segmentation of the overall plan into sections that are easily tested as is indicated to a moderate extent as shown by a mean of 2.71and 2.34 respectively.

4.5 Plan Maintenance

Table 4. 4: Extent that the steps undertaken to maintain the DR and BC plan

	No Extent at all	Small Extent	Moderate Extent	Large Extent	Very Large Extent	Mean	Stdev
Formal process for maintenance as your environment changes	2	10	21	33	33	3.82	0.2
Have an existing change management system to automatically update the DR plan	1	8	32	33	26	3.75	0.1
Provide a mechanism for regular review and evaluation on a pre-determined schedule	2	5	16	37	38	3.98	0.5
Establish agreements with critical vendors and service providers	2	10	15	29	44	4.03	0.4

The study sought to find out the extent that the steps were undertaken to maintain the DR and BC plan. According to the findings, establishing agreements with critical vendors and service providers to maintain the DR and BC plan was undertaken by the majority as shown by a mean of 4.03, providing a mechanism for regular review and evaluation on a pre-determined schedule was undertaken to a large extent as well as shown by a mean of 3.98. Formal process for maintenance as the company environment changes was undertaken to maintain the DR and BC plan as shown by a mean of 3.82 and lastly having an existing change management system to automatically update the DR plan was

undertaken to maintain the DR and BC plan as shown by a mean of 3.75. These findings are corroborated by Doughty (2005) who states that an organization needs to have both static reviews and dynamic reviews. A static review is a cyclical maintenance process whereby the business continuity plan at a predetermined point in time is reviewed. An annual review is a typical example of a static review regime while a dynamic reviews occurs when a strategic change occurs, for example, organizational restructure, integration of a new business.

4.6 Operating in Contingency Mode

Table 4. 5: Extent that following were considered in reference to operating in contingency mode

	No Extent at all	Small Extent	Moderate Extent	Large Extent	Very Large Extent	Mean	Stdev
Process descriptions	10	7	18	44	22	3.64	0.4
Minimum processing requirements	9	10	18	35	31	3.78	0.6
Identify location of vital records	2	9	26	19	44	3.94	0.7
Determine categories for vital records	2	10	20	26	41	3.91	0.1
Document critical forms	2	10	24	31	33	3.83	0.5
Document equipment - in the recovery site	2	13	24	41	20	3.64	0.4
Review of communication needs - in the recovery site	5	12	15	43	25	3.71	0.7
Software used in production	2	7	14	30	47	4.13	0.8
Production of logical drawings of communication and data networks during recovery	27	33	20	10	10	2.43	0.2
Review vendor list	18	36	32	9	5	2.47	0.4
Review of vendor restrictions	42	39	12	5	2	1.86	0.7
Software used in recovery	2	10	15	29	44	4.03	0.3

Criteria for returning to normal operating	5	11	21	48	14	3.52	0.3
Procedures for returning to normal operating mode	7	11	21	40	22	3.62	0.5
Procedures for recovering lost or damaged data	3	7	9	32	48	4.12	0.2

The study sought to find out the extent that following were considered in reference to operating in contingency mode. According to the findings, software used in production was indicated as the most important for a majority while working in contingency mode as is indicated by a mean of 4.13 followed by procedures for recovering lost or damaged data by a large number of the respondents as shown by a mean of 4.12. Majority of the respondents also undertook to factor in software used in recovery to a large extent as is shown by a mean of 4.03 followed by identifying location of vital records to a large extent as shown by a mean of 3.94 and also determination of categories of vital records to a large extent as shown by a mean of 3.91. Documenting critical forms was considered in reference to operating in contingency mode to a large extent as shown by a mean of 3.83 and consideration of the minimum processing requirements as shown by a mean of 3.78 followed by review of communication needs - in the recovery site to a large extent shown by a mean of 3.71. Procedures for returning to normal operating mode was also considered in reference to operating in contingency mode to a large extent as shown by a mean of 3.62 followed closely by a related activity referred to as criteria for returning to normal operating to a large extent as shown by a mean of 3.52. Lastly review vendor list was considered in reference to operating in contingency mode to a small extent as shown by a mean of 2.47 and production of logical drawings of communication and data networks during recovery was considered in reference to operating in contingency mode to a small extent as shown by a mean of 2.43 with review of vendor restrictions was considered the least in reference to operating in contingency mode to a small extent as shown by a mean of 1.86.

4.7 Benefits of Implementing DR and BCP

Table 4. 6: Extent the following were considered as benefits of having DR and BCP

	No Extent at all	Small Extent	Moderate Extent	Large Extent	Very Large Extent	Mean	Stdev
Competitive Edge	64	26	10	0	0	1.46	0.2
Reduction of Insurance Premiums	15	35	45	5	0	2.4	0.3
Improved understanding of the business is gained	6	4	18	70	12	4.08	0.5
Legal Compliance	9	28	55	4	4	2.66	0.4
Reduced inefficiencies	2	4	15	72	7	3.78	0.2
Reduced bureaucracy	74	14	2	10	0	1.48	0.1
Better Communication	16	24	37	18	5	2.72	0.3
Increase Value of Business	2	14	4	23	57	4.19	0.4
Risk Reduction	0	2	12	12	74	4.58	0.3
Increased customer confidence	4	67	23	2	4	2.35	0.5
Increased employee loyalty as their livelihoods are protected	4	65	22	5	4	2.4	0.3
BCM helped simplify complex processes	3	1	6	24	56	3.99	0.6
Reduced Downtime	6	4	12	24	64	4.66	0.1
Safeguard of Shareholder value	1	2	23	67	7	3.77	0.3
Minimize financial losses	1	1	32	64	2	3.65	0.2

The study sought to find out the extent certain as benefits were derived as a result of having DR and BCP. According to the findings, reduced downtime was considered as the benefit most derived from having DR and BCP to a very large extent as shown by a mean of 4.66, followed closely by risk reduction also by a very large extent as shown by a

mean of 4.58. Increased value of business was also strongly considered as benefits of having DR and BCP to a large extent as shown by a mean of 4.19, improved understanding of the business is gained was considered as benefits of having DR and BCP to a large extent as shown by a mean of 4.08. BCM helped simplify complex processes was considered as benefits of having DR and BCP to a large extent as shown by a mean of 3.99 and reduced inefficiencies also considered as benefits of having DR and BCP to a large extent as shown by a mean of 3.78. Safeguard of shareholder value was considered as benefits of having DR and BCP to a large extent as shown by a mean of 3.77, with minimizing financial losses considered to a large extent as shown by a mean of 3.65, better communication considered also to a moderate extent as shown by a mean of 2.72. Legal compliance was also considered a benefit of having DR and BCP to a moderate extent as shown by a mean of 2.66, followed by increased employee loyalty as their livelihoods are protected and reduction of insurance premiums was considered as benefits of having DR and BCP to a moderate extent as shown by a mean tie of 2.4. Increased customer confidence was also considered as benefits of having DR and BCP to a moderate extent as shown by a mean of 2.35, reduced bureaucracy was considered to a small extent as shown by a mean of 1.48, and lastly having a competitive edge was considered the least benefit of having DR and BCP as shown by a mean of 1.46. This findings confirm what Mikkelsen (2007) states that business continuity management involves creating resilient businesses; companies that are flexible and which can quickly identify and respond to challenges and threats. Belshaw (2008) had also stated the benefits of implementing BCP as amongst others revealing inefficiency, market edge, boosting staff morale, reduction of insurance premiums, and legal compliance.

4.8 Challenges of implementing DR and BCP

Table 4. 7: Rating of the challenges most experienced when implementing BC and DR

	No Extent at all	Small Extent	Moderate Extent	Large Extent	Very Large Extent	Mean	Stdev
Change of Project Sponsor	72	12	16	0	0	1.44	0.1
Change of Government	96	4	0	0	0	1.04	0.2
Difference in Work Culture Change	19	12	23	27	19	3.15	0.4
Conflict of interest in influential project stakeholders	23	4	42	15	15	2.92	0.2
Lack of senior management support	12	19	19	35	15	3.22	0.4
Identification of right stakeholders	8	8	8	42	35	3.91	0.6
Business reengineering challenges	5	11	23	42	19	3.59	0.1
Delay in Payments	3	9	29	44	15	3.59	0.4
Beauracracy	2	5	15	43	35	4.04	0.2
Government Interference	71	24	3	2	0	1.36	0.3
Procurement delays	0	8	8	62	23	4.03	0.6
Corruption	35	42	18	5	0	1.93	0.8
Incomplete requirements	8	8	45	35	4	3.19	0.2
Poor supervisory	8	42	35	8	8	2.69	0.1

The study sought to find out how the respondents rated the challenges most experienced when implementing BC and DR. According to the findings, beauracracy was considered the greatest challenge when implementing BC and DR to a large extent as shown by a mean of 4.04 followed closely by procurement delays to a large extent as shown by a

mean of 4.03 and identification of right stakeholders to a large extent as shown by a mean of 3.91. Business reengineering challenges and delays in payments was experienced when implementing BC and DR to a large extent as shown by a mean tie of 3.59, lack of senior management support experienced to a large extent as shown by a mean of 3.22. Incomplete requirements was experienced as a challenge when implementing BC and DR to a moderate extent as shown by a mean of 3.19 followed by differences in work culture change to a moderate extent as shown by a mean of 3.15. Conflict of interest in influential project stakeholders was experienced when implementing BC and DR to a moderate extent as shown by a mean of 2.92 followed by poor supervisory to a moderate extent as shown by a mean of 2.69. Amongst the least experienced challenges when implementing BC and DR was corruption to a small extent as shown by a mean of 1.93, change of project sponsor to a small extent as shown by a mean of 1.44, government interference to a small extent as shown by a mean of 1.36 and lastly change of government was least experienced when implementing BC and DR to a large extent as shown by a mean of 1.04.

CHAPTER FIVE

SUMMARY OF THE FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

The chapter provides the summary of the findings from chapter four, and it also gives the conclusions and recommendations of the study based on the objectives of the study. The objectives of this study were to investigate the disaster recovery and business continuity plans of class-A parastatals in the various government ministries.

5.2 Summary of the Findings

The study aimed at investigating the implementation of disaster recovery and business continuity plans of class-A parastatals in the various government ministries. At the pre-planning phase the study found that majority of the respondents undertook performing a risk management review to identify and correct obvious weaknesses to a large extent as shown by a mean of 3.42. This can be attributed to the fact that BCP is a measure of reducing risks and hence the need to perform a risk management review. To a large extent many respondents also reported to have used an industry standard disaster recovery (DR) methodology in addition to performing a Business Impact Assessment (BIA) to prioritize the business processes to a moderate extent as shown by a mean of 2.59 and preparation of a recovery options list that itemizes recovery options by business process to a small extent as shown by a mean of 2.41. At the development phase the steps most parastatals found to be most important when developing BC plan the organization were developing a formal system backup policy and schedule to a large extent as shown by a mean of 4.03, designation a location of backup tapes to a large extent as shown by a mean of 3.99, document emergency response procedures to occur during and after an emergency to a large extent as shown by a mean of 3.98, inventory of assets needed for offsite recovery to a large extent as shown by a mean of 3.62, list of detailed tasks needed for offsite recovery to a large extent as shown by a mean of 3.54, and definition of a call tree for notifying staff when a disaster is declared to a large extent as shown by a mean of 3.54.

At the plan testing stage the study found that most parastatals undertook various steps during the testing of the plan key among them having frequently scheduled tests as indicated to a large extent by a mean of 3.98, establishing a formal process to certify the success of tests to a large extent as shown by a mean of 3.9, development of a test plan to a large extent as shown by a mean of 3.82, establishment of testing success indicators in the test plan and testing of remote office connectivity as a success indicator both shown by a mean of 3.52, and finally total time for execution of recovery tasks as well as testing of restored systems as a success indicator to a large extent as shown by a mean of 3.52. During the plan maintenance phase establishing agreements with critical vendor and service provider was undertaken to maintain the DR and BC plan as shown by a mean of 4.03, provide a mechanism for regular review and evaluation on a pre-determined schedule was undertaken to maintain the DR and BC plan as shown by a mean of 3.98, formal process for maintenance as your environment changes was undertaken to maintain the DR and BC plan as shown by a mean of 3.82 and have an existing change management system to automatically update the DR plan was undertaken to maintain the DR and BC plan as shown by a mean of 3.75.

In reference to operating in contingency mode the study established that procedures for recovering lost or damaged data was considered in reference to operating in contingency mode, production of logical drawings of communication and data networks during recovery was considered in reference to operating in contingency mode, review vendor list was considered in reference to operating in contingency mode, identify location of vital records was considered in reference to operating in contingency mode, review of vendor restrictions was considered in reference to operating in contingency mode, review of communication needs - in the recovery site was considered in reference to operating in contingency mode, software used in recovery was considered in reference to operating in contingency mode, determine categories for vital records was considered in reference to operating in contingency mode and document critical forms was considered in reference to operating in contingency mode.

Among the benefits derived from implementing BCP and DR reduced downtime was considered as the greatest benefit derived from implementing BC and DR plans as was indicated by a mean of 4.66. Others ranked highly by almost all the respondents were improved understanding of the business is gained to a very large extent, increase value of business to a very large extent, improved understanding of the business is gained was derived to a very large extent. Others derived though to a small extent included better communication, increased employee loyalty as their livelihoods are protected as well as legal compliance all to a moderate extent. As for challenges when implementing BC and DR plans change of project sponsor was experienced when implementing BC and DR to a large extent, corruption was experienced when implementing BC and DR to a large extent, government Interference was experienced when implementing BC and DR to a large extent as shown by a mean of 4.27, incomplete requirements was experienced when implementing BC and DR to a large extent, procurement delays was experienced when implementing BC and DR to a large extent, change of Government was experienced when implementing BC and DR to a large extent, identification of right stakeholders was experienced when implementing BC and DR to a large extent and poor supervisory was experienced when implementing BC and DR to a large extent.

5.3 Conclusions

The study concludes that almost all class-A parastatals have employed some form of disaster recovery and business continuity planning mechanisms which highlights the importance of ensuring continual service delivery and minimizing interruptions and loss of data. This was previously something done by the private sector but has now been completely adopted by the public sector namely parastatals. The study also concludes that majority of respondents seemed to embrace almost all the steps in the various sections of BC and DR planning. During the pre-planning phase performing a business impact assessment to prioritizing business processes, consulting business process owners during the business impact assessment and performing a risk management review to identify and correct obvious weaknesses was considered the most important steps for the majority of respondents followed by adopting an industry standard disaster recovery methodology

with preparation of a recovery options list that itemizes recovery options given least significance.

During plan developing majority of the respondents had formal system backup policy and schedules as well as designation of backup tapes were given highest priority. This is because it is through having this backup policy that backups can be performed and tested thus ensuring they are successful. It is also important that there is documentation of emergency response procedures to occur during and after an emergency. Inventory of the assets needed for offsite recovery is also very important. During plan testing phase it is important to have frequently scheduled tests in order to ensure test results are up-to-date and successful. Parastatals should have a formal process to certify the success of tests, establishment of testing success indicators in test plans as well as testing of remote office connectivity as a success indicator. Least in the priority of most respondents was having an independent observer to validate test results which should be given more priority to ensure test results are evaluated independently.

During plan maintenance was establishing agreements with critical vendor and service provider followed by providing a mechanism for regular review and evaluation on a pre-determined schedule. Likewise formal process for maintenance as the environment changes and having an existing change management system to automatically update the DR plan were also highly considered. In reference to operating in contingency mode software used in production, procedures for recovering lost or damaged data, software used in recovery, identification of vital records, determination of categories of vital records, documentation of critical forms as well as consideration for minimum processing requirements were considered. The greatest benefits derived from having DR and BCP were reduced downtime, risk reduction, increased value of business, improved understanding of the business, simplification of complex processes, reduction of inefficiencies, safeguard of shareholder value and finally minimizing financial losses. The challenges experienced by most were beauracracy, procurement delays, identification of right stakeholders, delay in payments and finally business reengineering challenges.

5.4 Recommendation

The study recommends that majority of parastatals should perform a Business Impact Assessment (BIA) to prioritize the business processes; consult business process owners during the business impact assessment and perform a risk management review to identify and correct obvious weaknesses during the pre-planning phase. This not only ensures that the initial phase is successful but that the process is an all-inclusive process with the users from other departments getting involved. Though the step was not considered very important parastatals should also use industry standards methodologies as they are tried and tested over time.

The study recommends organizations should develop formal system backup policies and schedules as well as designate a location for backup tapes. In addition it is important that emergency response procedures to occur during and after emergencies. Although most respondents did not see the need to have a public relations team to address external inquiries the study recommends that parastatals give this more consideration given the fact that they are public entities and as such there operations affect a very large portion of the population thus the need to address citizens' concerns should be given more priority. In addition although parastatals are guided by public procurement and disposal act it is important that they get vendors' approval to be included in their BCP so as to avoid back passing and unnecessary delays during emergencies.

The study recommends that parastatals should have frequently scheduled tests in their test plans and a formal process to certify the success of the testing. Although given least priority it is important for parastatals to have independent observers to validate the test results as it makes the test objective and results more credible given that it is an unbiased observer. Also, parastatals should have agreements with critical vendors and service providers as this quickens the recovery process as the vendors are under contract to deliver either the service or product required for recovery e.g. a hard disk. Parastatals should also have the software used in production kept in contingency mode to aid in recovery and restoration. It also recommends that procedures for recovering lost or damaged data be put in place so that the process is carried out in a consistent and

organized documented manner thereby minimizing the loss of data. Although not highly considered review of vendor restrictions is important as it enables the organization to know what the vendor can or cannot do thereby minimizing unpleasant surprises e.g. expecting the vendor to deliver a server when they can only deliver hard disks under the circumstances.

5.5 Recommendation for Further Studies

This study has reviewed the study on the disaster recovery and business continuity plans of class-A parastatals in the various government ministries. To this end further research is recommended in the implementation of the same in the other parastatals in class-B and class-C. Likewise in this era of cloud computing there is need for research on how cloud computing affects implementation of disaster recovery and business continuity plans in both the private and public sectors.

REFERENCES

Gay, C (2007). Emergency Notification and Escalation Systems**.** *Disaster Recovery Journal. 1 (*20), 53-57.

Smith, D., & Laman, S. (2010). *Prevent a Document Catastrophe with Proactive Disaster Recovery Planning*. Disaster Recovery Journal, 23(2), 60-61.

Chow, F (2007). *How Risk Assessment Works with Success.* Disaster Recovery Journal, 20 (1), 41-42.

Disaster Recovery. (2011). *Disaster Recovery.* Retrieved from http://www.disasterrecovery.org/disaster_recovery.html

Ward, J & Peppard J. (2002). *Strategic Planning for Information System.* New York: John Wiley & Sons, Inc.

Drucker, P. (1974). Management: tasks, responsibilities and Practices. New York: Harper and Row.

Hiles, A. (2003). *Business Continuity: Best Practices-World Class Business Continuity Management.* Rothstein Associates, Inc.

Myers, K. (1993). *Total Contingency Planning for Disasters.* New York: John Wiley & Sons, Inc.

Cooper, R & Schindler, P. (2003). *Business Research Methods.* New York: McGraw Hill International.

Mugenda, M., & Mugenda, G (2003). *Research methods: Quantitative and qualitative*

approaches. Nairobi, Kenya: Act Press.

Laye, J. (2002). *Avoiding Disaster: How to keep your business going when catastrophe strikes*. New York: John Wiley & Sons, Inc.

Doughty, K. (2005). *Building Maintenance Processes for Business Continuity Plans*. Auerbech Publications.

Okolita, k. (2009). *Building an Enterprise-Wide Business Continuity Program* Retrieved from CSO Security and Risk website: http://www.csoonline.com/article/509539/how-to-perform-a-disaster-recovery-business-impact-analysis

Mikkelsen, M (2007, January 12). *The Business Benefits of Business Continuity.* Retrieved from http://www.continuitycentral.com/feature0427.htm

Wilder, D (2008, October 06). *The New Business Continuity Model.* Retrieved from http://www.talkingbusinesscontinuity.com/downloads/pdf/The-New-Business-Continuity-Model.pdf

Singh, D. (2009, June 01). *Myriad Challenges in executing Government Projects in Developing Countries*. Retrieved from http://www.theicpm.com/blogs/non-specific-pm-topics/3235-myriad-challenges-in-executing-government-projects-in-developing-countries

Slater, D. Hager. (2009, December 09). *How to Perform a Disaster Recovery Business Impact Analysis.* Retrieved from http://www.csoonline.com/article/509539/how-to-perform-a-disaster-recovery-business-impact-analysis

Belshaw, S. (2008, September 08). *10 Reasons to Have a Business Continuity Plan.* Retrieved from http://www.fpb.org/hottips/179

Federal Office for Information Security (BSI). (2009). *BSI-Standard 100-4: Business Continuity Management* (1st ed.). Bonn,Germany: Author.

Gartner Research. (2001). Business Continuity and Disaster Recovery Planning and Management: Perspective. Retrieved from http://www.availability.com/resource/pdfs/DPRO-100862.pdf

Juniper Networks Inc. (2009). *Ensuring Business Continuity in Government.* Retrieved from http://www.juniper.net/us/en/local/pdf/whitepapers/2000203-en.pdf

Janco Associates Inc. (2011). *DRP and BCP Best Practices: Proper DR BC Planning required for successful recovery.* Retrieved from http://e-janco.com/DisasterPlanningBuinessContinuityBestPractices.htm.

Protiviti Independent Risk Consulting. (2006). *Guide to Business Continuity Management.* Retrieved from http://www.knowledgeleader.com/KnowledgeLeader/content.nsf/Web+Content/WhitePapersArticlesBCMFAQGuide!OpenDocument.

Office of The President, Directorate of Personnel Management. (2006). *Handbook for Civil Service Staff Induction.* Retrieved from http://www.dpm.go.ke.

State Corporations Advisory Committee. Retrieved from http://www.scac.go.ke/ on August 23rd 2011.

BUSINESS CONTINUITY AND DISASTER RECOVERY IMPLEMENTATION QUESTIONNAIRE

This questionnaire has been designed to assist the researcher collect data concerning Business Continuity and Disaster Recovery Implementation in State Parastatals. You have been identified as one of the respondents in this study. Section A: contains questions on profiling, Section B: The process of BCP and DR implementation, Section C- The benefits of implementing BCP and DR and lastly Section D- Challenges faced in implementing BCP and DR. 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 gender? Male [ ] Female [ ]

2. Your age bracket?
   Below 20 yrs [ ] 31-35 yrs [ ] 46-50 yrs [ ]
   21-25 yrs [ ] 36- 40 yrs [ ] Over 50 yrs [ ]
   26-30 yrs [ ] 41-45 yrs [ ]
3. Kindly indicate you current level of education?

   Secondary [ ] College [ ] Graduate degree [ ]
   Post graduate degree [ ] Others (Please specify……)

4. What is your designation in the organization?
   IT Manager [ ] Business Analyst [ ] Network & Sys Admin [ ]
   IT officer [ ] Others (please specify…….)

5. For how long have you worked in your organization?

Less than 5 yrs [ ]	16-20yrs [ ]	Over 30 yrs [ ]
5-10 yrs [ ]	21- 25 yrs [ ]	
11-15 yrs [ ]	26-30 yrs [ ]	

SECTION B:

This section covers the implementation aspect of the Disaster Recovery and Business Continuity Plan

PRE PLANNING

No	To what extent were the following steps undertaken during the pre-planning phase	1 No Extent at all	2 Small Extent	3 Moderate Extent	4 Large Extent	5 Very Large Extent
1.	Industry standard disaster recovery (DR) methodology					
2.	Perform a Business Impact Assessment (BIA) to prioritize your business processes					
3.	Consult business process owners during the BIA					
4.	Perform a risk management review to identify and correct obvious weaknesses					
5.	Preparation of a recovery options list that itemizes recovery options by business process					

PLAN DEVELOPMENT

No	To what extent were the following steps taken when developing the organization DR and BC plan	1 No Extent at all	2 Small Extent	3 Moderate Extent	4 Large Extent	5 Very Large Extent
1.	Develop a disaster organization chart that defines recovery teams					
2.	Define a call tree for notifying your staff when a disaster is declared					
3.	Consideration been given to					

	developing the BC plan around a worst case scenario					
4.	Measures to manage contingency processes while your IT systems are being recovered					
5.	Understand the company time and data requirements (e.g. how much downtime can the company afford)					
6.	Appoint a public relations team to address external inquiries					
7.	Develop a key vendors contact list					
8.	Vendors' approval for their inclusion in your plan (e.g., will they be available, under contract, etc.)					
9.	Inventory of assets needed for offsite recovery (example: backup tapes, operating system software etc.)					
10.	Document emergency response procedures to occur during and after an emergency					
11.	Formal system backup policy and schedule					
12.	Designate a location of backup tapes					
13.	List of detailed tasks needed for offsite recovery					
14.	Investigate new advanced technologies that can reduce downtime					

PLAN TESTING

No	To what extent are the following test plans in the DR and BC Plan	1 No Extent at all	2 Small Extent	3 Moderate Extent	4 Large Extent	5 Very Large Extent
1.	Development of a test plan					
2.	Segmentation of the overall plan into sections that are easily tested					
3.	Frequently scheduled tests					
4.	Use of incidents as a form of testing					
5.	Establishment of testing success indicators in the test plan					
6.	Total time for execution of recovery tasks as a success indicator					
8.	Testing of remote office connectivity as a success indicator					
9.	Testing of restored systems as a success indicator					
10.	Formal process to certify the success of your testing e.g. Test results documentation					
11.	Independent observer to validate the test results					

PLAN MAINTENANCE

No	To what extent are the following steps undertaken to maintain the DR and BC plan	1 No Extent at all	2 Small Extent	3 Moderate Extent	4 Large Extent	5 Very Large Extent
1.	Formal process for maintenance as your environment changes					
2.	Have an existing change management system to automatically update the DR plan					
3.	Provide a mechanism for regular review and evaluation on a pre-determined schedule					
4.	Establish agreements with critical vendor and service provider					

OPERATING IN CONTNGENCY MODE

No	To what extent are the following considered in reference to operating in contingency mode	1 No Extent at all	2 Small Extent	3 Moderate Extent	4 Large Extent	5 Very Large Extent
1.	Process descriptions					
2.	Minimum processing requirements					
3.	Identify location of vital records					
4.	Determine categories for vital records					
5.	Document critical forms					
6.	Document equipment - in the recovery site					
7.	Review of communication needs - in the recovery site					

8.	Software used in production					
9.	Production of logical drawings of communication and data networks during recovery					
10.	Review vendor list					
11.	Review of vendor restrictions					
12.	Software used in recovery					
13.	Criteria for returning to normal operating					
14.	Procedures for returning to normal operating mode					
15.	Procedures for recovering lost or damaged data					

SECTION C

BENEFITS

Please indicate if your organization has derived any of the benefits listed after implementation of DR and BCP

No	**To what extent do you consider the following as benefits of having DR and BCP**	**1 No Extent at all**	**2 Small Extent**	**3 Moderate Extent**	**4 Large Extent**	**5 Very Large Extent**
1.	Competitive Edge					
2.	Reduction of Insurance Premiums					
3.	Improved understanding of the business is gained					
4.	Legal Compliance					
5.	Reduced inefficiencies					
6.	Reduced bureaucracy					
7.	Better Communication					

8.	Increase Value of Business					
9.	Risk Reduction					
10.	Increased customer confidence					
11.	Increased employee loyalty as their livelihoods are protected					
12.	BCM helped simplify complex processes					
13.	Reduced Downtime					
14.	Safeguard of Shareholder value					
15.	Minimize financial losses					

Others

……
……
……
……
……
……
……
……
……

SECTION D

Which of the following would you rate as the challenges most experienced when implementing BC and DR:

No		1 No Extent at all	2 Small Extent	3 Moderate Extent	4 Large Extent	5 Very Large Extent
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.	Beauracracy					
10.	Government Interference					
11.	Procurement delays					
12.	Corruption					
13.	Incomplete requirements					
14.	Poor supervisory					

Others

……
……
……
……
……
……
……

APPENDIX

Guidelines on Terms and Conditions of Service for State Corporations', Chief Executive Officers, Chairmen and Board Members, Management Staff, Unionisable Staff……..23rd November, 2004.

Permanent Secretary, Secretary to the Cabinet and Head of Public Service….Ref No: OP/CAB.9/21/2A/LII/43

NO	PARASTATAL	SECTOR
1.	Kenya Revenue Authority	Financial
2.	East African Portland Cement Co	Commercial/Manufacturing
3.	Kenya Electricity Generating Co	
4.	Kenya Pipeline Co	
5.	Kenya Power & Lighting Co	
6.	Telkom Kenya Ltd	
7.	Postal Corporation of Kenya	
8.	Capital Markets Authority	Regulatory Corporations
9.	Communications Commission of Kenya	
10.	Electricity Regulatory Board	
11.	Retirement Benefits Authority	
12.	Kenya Agricultural Research Institute	Training and Research Institutions
13.	Kenya Institute of Public Policy Research And Analysis	
14.	Higher Education Loans Board	Service Corporations
15.	Kenya Accounts and Secretaries National Examinations Board	
16.	National Hospital Insurance Fund	
17.	Teachers Service Commission	
18.	National Social Security Fund	