5-2019

Developing a Business Continuity and Disaster Recovery Plan: Kenya State Organizations

Manas Byadigera
mbyadigera@stcloudstate.edu

Developing a Business Continuity and Disaster Recovery Plan: Kenya State Organizations

by

Manas Byadigera

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree

Master of Science in

Information Assurance

May, 2019

Starred Paper Committee:
Susantha Herath, Chairperson
Sneh Kalia
Lynn Collen

Abstract

Business Continuity and Disaster Recovery planning are one of the crucial constituents in a business organization but ignored mostly. Data relatively without any assistance has become an important factor to success in organizations. Using massive databases, organizations can make necessary prudential and active resolution giving them an aggressive edge in the global market. Organizations are now successful with their businesses only if they can deploy a proper business continuity and a disaster recovery plan which depends largely on the organization's knowledge and understanding over different disciplines of disasters such as human errors, software failures, hardware failures, and natural disasters. This study mainly gives us an idea about various business continuity and disaster recovery mechanisms of Class A parastatals government agencies. Here are survey results from various low-level and high-level government employees of Kenya with certain questionnaires for which we have statistical data and provide few proposals of how Class A parastatals in Kenya can improvise in designing and deploying a disaster recovery plan which will help in business continuity and quicker recovery whenever they face a disaster.

Acknowledgments

I want to thank and express my gratitude to everyone who has helped in the completion of my Starred Paper. Firstly, I would like to thank Dr. Susantha Herath, the chairperson of my Starred Paper Committee who helped through the completion of my research study by providing guidance required. I would also like to thank other faculty members in my committee, Dr. Lynn Collen and Dr. Sneh Kalia for their guidance and support in my study. I want to thank Dr. Lynn Collen for her insightful comments which helped me in my research study.

Thanks to my parents and dearest ones in encouraging me and motivating me towards completing my Starred Paper successfully.

Finally, I would like to thank the St. Cloud State University library staff and resources which have assisted me during my research study. This paper would have been quite impossible without any support received from the above mentioned.

Table of Contents

Chapter Page

Chapter Page

List of Tables

List of Figures

Chapter 1: Introduction

Introduction

In today's era, several organizations around a focus on the software side development which makes them think that technology and applications are one of the important components that lead an organization to success. With this in their mind, organizations consider many software IT professionals, high-end infrastructure, and updated technology, electronic equipment, and applications. Similarly, Kenya has started moving towards developing in Information, Communication and Technology (ICT) as their main aspects. With the development in the Information Technology and Applications, one can see that internal and external attack factors have entered the organization to bring down businesses or try to extract confidential information from the organization. Every attack happening has its effects on the organization with different impacts on their businesses and assets. Also, one can see that the internet has now been given preference as the first point of contact for developing businesses or using technology and applications in an organization. Any interruptions on the internet would, therefore, cause disruptions in the organization activities and performances.

As one can see from what can interrupt the business processes, organizations must ensure the protection of assets, information and enhance proper disaster recovery/business continuity plans. Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) are the main contingency plans carried out separately in different time horizons within organizations (Wunnava, 2011). Business Continuity Plans refers to a pre-planned event which could bring in continued processes or resume certain functions to a satisfactory level after the impact of the disaster on an organization. Disaster Recovery refers to recovering assets, information and other important aspects of an organization and bring back the functioning of a business/organization to

its normal condition. Organizational Resilience is one of the trends today in the eye of professionals. This means that it enquires organizations to develop effective plans for both short-term resuming (BCP) and long-term restoration (DRP) of their disrupted operations following disruptive events (Riolli, (2003). This study aimed to analyze the Class A parastatals survey statistical data retrieved using a set of questionnaires and answers given by mid-level and senior-level professionals of government agencies of Kenya, and provide recommendations of developing business continuity and disaster recovery plans. It also brings up awareness among the students and employees how to protect themselves or respective institutions and organizations from disasters like human errors, hardware and software failures and natural disasters.

Though Kenya is one of the biggest and advanced cities of Africa, one can still see that its performance on the economy is poor which means it has low GDP and is mostly attracted due to tourism, telecommunication, and agriculture aspects which brings in a strong point for businesses there. One can also see that child labor is very much common in Kenya which brings down the percentage of literacy there. Due to this low literacy percentage, one can estimate to what extent business continuity and disaster recovery planning could mean to them. Disaster Management is very poor in Kenya due to the costs they must incur for disaster management. Kenya has been one of the most prone areas to natural disasters like droughts, fires, floods and human errors like industrial incidents and terrorist/human activities. There must thus bring in awareness and cost-effective disaster management plans to protect assets, resources and confidential information in respective government and private educational institutions and business organizations.

Problem Statement

The extent to which parastatals have focused on disaster management measures are known through a previous survey done using mid-level and senior-level employees feedbacks, but the main challenge is while preparing a business continuity and disaster recovery plan, these organizations always strived hard to develop easily accessible and cost-effective plans to protect themselves from unwanted-unexpected events.

Nature and Significance of the Problem

In Kenya, several parastatals and organizations have ignored to produce analysis on disasters and prepare disaster management plans, and this was because they have here called every unexpected event to mostly be an act of nature like floods, droughts, earthquakes, and other similar actions. They've always tried to escape from disaster management concepts as it incurs several costs involved in it. Since the use of internet and technology has increased in Kenya and around the world, one can say that human errors and software errors like hacking, power down, malicious acts, viruses can cause huge disruptions and damage to data and assets/resources in an organization.

Parastatals thus consist of highly sensitive data, and confidential information which is retrieved from computer systems and databases are maintained in there. The information and data are mandatory for the parastatals as that is what is necessary for them in their businesses for providing effective support and services to the users and customers. So, for all the operations to take place continuously without disruptions, one can see a necessity to consider and plan for disaster recovery mechanisms and business continuity plans to ensure the protection of assets and resources and have back-ups for information/data.

As there is rapid growth in technology, applications and use of internet around the world, one can see that organizations cannot ignore the concept of business continuity and disaster recovery plans by not having a proper contingency plan. BC and DR plans enhance the responsiveness and guarantee that sensible choices are made by employees during emergencies by providing composed and hazel-free techniques to encounter a disaster (Gregg, 2009). Business continuity plan in government is a need to ensure that essential functions can continue during and after a disaster (Juniper, 2009). Government organizations must importantly focus on protecting sensitive, high-end and confidential data and information since they will have large databases and can use minimal-cost methods to protect them from external and internal attacks in the form of either human activities or natural activities.

There are some common misconceptions for not having business continuity plans (Batson, 2017):

1. Insurance covers losses;
2. One knows completely what to do in an emergency;
3. I don’t have time to develop a BC plan.

Here are Batson’s thoughts about them which are very much true regarding the above-mentioned misconceptions (Batson, 2017),

Firstly, insurance does cover losses, but there are a few more risks that insurance does not cover such as death, federal violations, liability and loss of reputation.

Second, everyone has a general idea of what to do in an emergency, but unless you have previously had your building destroyed by a tornado, then you probably don’t know how to deal with the aftermath. Also, when an emergency strikes there are several waves of panic. Everyone

handles situations differently and having a plan in place can help to keep everyone on the same page so that the situation can be handled in a calm and collected manner.

Third, you might not have time to create a business continuity plan, but lucky for you, some companies and professionals can help you and have the time and expertise to do it.

As per the above information, they are ignoring business continuity and disaster recovery is easy but difficult to address the issues that would mandatorily require the use of a professional-developed disaster management strategy or plan which could help them at the time of difficulties where any resources cannot help them in regaining their processes and resume their operations. The study will help bring out awareness through education, best practices, and active training and deployment activities and produce the necessity of disaster recovery planning (DRP) and business continuity planning (BCP) and provide cost-effective mechanisms in terms of protecting information, location, infrastructure, access control, and efficient back-ups.

Objective of Research

The main objective of our study is to research the issues which are causing concerns in the implementation of business continuity planning and disaster recovery planning and then produce efficient and effective ways to bring awareness and prepare-deploy both business continuity and disaster recovery plans.

Study Questions and Hypothesis

1. What are the business continuity and disaster mechanisms developed by Class A parastatals in Kenya?
2. How can awareness be brought in towards disaster management at educational institutions, government ministries, and private organizations in Kenya?

3. What practices can be used to create and implement business continuity and disaster recovery plan? How can the plan be reliable, maintained and what cost-effective and easy-accessible mechanism implemented in the small-scale/large-scale organizations?

Definitions of Terms

ICT: Information, Communication, and Technology.

BC: Business Continuity.

DR: Disaster Recovery.

BCP: Business Continuity Planning.

DRP: Disaster Recovery Planning.

IT: Information Technology.

ISO: International Standards for Organizations.

BIA: Business Impact Analysis.

Summary

This section has thus covered up the introduction towards our research on Business Continuity and Disaster Recovery planning, bringing awareness using educational and implementable processes and help in the maintenance of a proper and well-designed/well-developed disaster management plan. This study would help many professionals and managers working with this respective department and enhance or support the necessity for business continuity and disaster recovery planning. This study can also be picked as a reference to future studies. This study also gives importance to backing up information over the cloud using various cloud services where there could be huge scope for research and this study can be used a reference.

Figure 1, below, describes the basic components of disaster management in every organization. These three components are always one of the important things to concentrate on while planning on documenting and creating disaster management in a state organization or private organization. From Figure 1, you can know that the three components here are discussed in disaster management and they are:

1. Business Continuity Plan (BCP)
2. Disaster Recovery Plan (DRP)
3. Back and Recovery Procedures: This includes the backup procedures which you can refer to off-site storages of data like Tape, Hard Drives, etc. and on-site storages like cloud services, hybrid cloud, direct-to-cloud backup. Their respective data recovery methods can be inferred to as:

Recovering data from the local devices in the organization. Here, one would generally look to speak about virtual machines that are installed on the computer systems where data can be backed up, and all the processes can continue from the devices like applications, settings, etc.

Recovering data from the cloud used by organizations. This would mean to extract data from the cloud over the internet. Sometimes this can be too time-consuming because of the large size of data one deals within organizations (GB/TB) and will have to look for better cloud services where one will be able to deal with big data easily and comfortably.

Recovering data right in the cloud. In some organizations, there is a service called "Disaster Recovery as a Service" (DRaaS) which would allow us to continue our processes through the cloud without many efforts by downloading a large amount of data into the computer system which consumes much space.

Figure 1: Basic disaster management concepts (Rutledge, 2014)

Therefore, from the above information regarding Figure 1, one can understand what the important components of a disaster management approach in an organization are. Business Continuity Planning and risk assessments, Disaster Recovery Planning with test drills and data backup and recovery procedures will help a company ensure survivability in this dangerous world of disasters (Rutledge, 2014).

Chapter 2: Background and Review of Literature

Introduction

The Internet has nowadays become one of the most important sources for every type of organization to run their businesses. Social media websites like Facebook, Instagram, Twitter, G-mail, Yahoo mail, Snapchat, LinkedIn, etc. have become so popular that you can easily see millions of accounts created in these websites where some personal information must be produced to them. If there is any kind of disturbance created, all the information on these websites can be compromised and lost. To add to these issues, they also have mobile applications linked with each website and other applications like WhatsApp, IMO, Skype, etc. which also stores some personal information of ours and can be compromised if any interference has been created. That was just an example of how information can be compromised and hence calls for high-level security levels and proper business continuity and disaster recovery plans.

Many a time, people do have misconceptions about Disaster Recovery Planning and Business Continuity Planning, but both terms are quite different in comparison to each other. This chapter would give us an idea about the types of disasters happening around the world and with a focus on Kenya. Here would also be a discussion about Business Continuity and Disaster Recovery in brief and define the parastatals in Kenya. One would also see why Kenya has been chosen our choice of interest to my study in this research. The main advantage of Disaster Recovery and Business Continuity was try minimizing the organization downtime, but Kenya had other reasons for not trying to properly focus on Disaster Management and hence will be discussed what plans they can make shortly for minimal security, protection, and preparation.

Background Related to the Problem

One of the major happenings around the world includes Disasters. These unexpected events always take place without anyone's knowledge and make a sudden impact which is quite big and damages many assets, information, and resources. Any disturbances caused by nature or human in an organization or any area which causes damage to resources, information, people, and assets can be termed as a Disaster. One can mainly see that there are two types of disasters like Natural Disasters and Human-Made Disasters.

Table 1

Types of Disasters (Milledge, 2015)

TYPES OF DISASTERS TWO TYPES: NATURAL AND MAN-INDUCED	
Natural Disasters	Man-Induced Disasters
1. Wind - Cyclone, Storm, Tidal Waves 2. Water - Flood, Cloud Burst, Cold Wave, Heat Wave, Flash Flood, Drought 3. Earth - Earthquake, Landslides, Tsunami	1. Accidents: Rail, Road, Air, Sea, Building Collapse 2. Industrial Mishaps: Gas Leak, Explosion 3. Fire - Building, Coal Mines, Oil Fields 4. Forest Fire – Mainly Tropical Countries 5. Contamination/Poisoning – Food, Water, Illicit Liquors 6. Terrorist Activities 7. Ecological – Pollution (Air, Water, Noise) Sea Level Rise 8. Social: War, Riots, Hijacking, Civil Unrest

Table 1 above describes us about the important classification in the types of disasters which are Natural and Man-made. One can easily know that natural disasters would be referred to disturbances in water, land, and wind like storms, tornadoes, high-level waves, earthquakes, etc. Table 1 also shows us the various kinds of human-made disasters like road accidents, contamination incidents, wars, hijacking, terrorist activities, leakages in industries like chemicals, gas, etc. and disturbances at oil fields, coal mines, etc. Human-induced disasters are always variable and do not have a specific time of occurrence.

Based on reports, 43% of companies influenced by severe disasters never reopened, and about 30 % of them failed within two years (Virginia Cerullo, 2004). It can also be inferred that both natural and human-made disasters have an equal effect around the world. Though natural disasters cannot be well defended, one can put in full efforts towards human-made disasters or human errors in an organization. Organizations are nowadays facing mostly disasters caused by human errors.

Figure 2 describes the percentage of various disasters happening around the world. Which one do you think weighs the most? The part called "Other" weighs the most in the percentage of disasters happening around the world. Other refers to human-made or human-induced disasters which could now make us understand that disasters caused by human are more around and thus could be tried to bring down or give enough protection and backup so that one could decrease that percentage where humans are involved in incidents happening around. Figure 2 gives us a brief idea about how far are human-made disasters when compared to natural disasters and should thus bring down awareness to decrease human-made errors that effects resources, assets, information and people. Maybe natural disasters cannot be controlled, but human-made disasters can be controlled to the most extent.

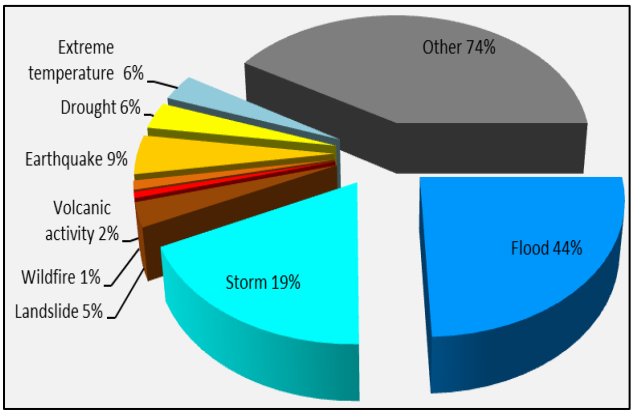

Figure 2: Percentage of disasters around the world (Gahler, 2016)

Figure 2 above shows us what effects disasters are making around the world in terms of natural and human-made. The impact of disasters on the environment has become more severe over the last decades. Moreover, the reported number of disasters has dramatically increased, as well as the costs to the global economy and the number of people affected (Gahler, 2016). Kenya also faces low economy and hence did not focus on disaster management.

To develop a contingency plan for an organization or a selected area, preparation and planning are divided into three phases:

1. Incidence Response (IR).
2. Disaster Recovery Planning (DRP).
3. Business Continuity Planning (BCP).

Incident response can be simply defined as the processes or procedures used to be implemented after an act of disaster in an organization and control the impact of the disaster. One can also have an Incident Response team where they are the workers who plan, prepare and deploy their actions into the situation as soon as the disaster has made its impact.

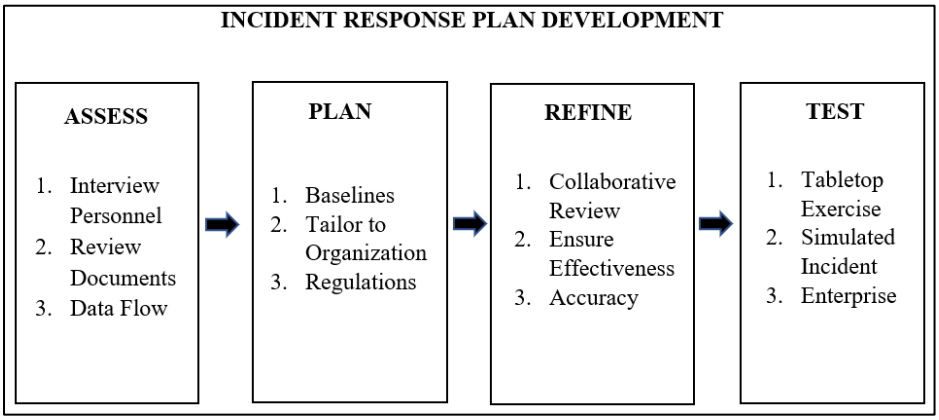

Figure 3: Incident response plan development in organization (CyberSponse, 2017)

From Figure 3, there are four important steps to be considered in an incident response plan development:

1. Assess;
2. Plan;
3. Refine;
4. Test.

According to CyberSponse Crew, they say that all businesses are different, and their recommendations are as follows (CyberSponse, 2017):

1. You need first to embrace and create an incident response team, available 24/7, to manage direct and facility any cybersecurity or business continuity incident.
2. Train your team. If they do not know what incident response is, there is a ton of resources online to do this. Hold weekly sessions to whiteboard plans, ideas, talk about technology, what is changing and so on. Get your team used to the idea that threats/alerts/incidents cost the company money, and why a consistent and effective response is required.
3. Carry out a thorough analysis and identify critical assets, key terrains and areas to most protect within the businesses. What sort of information security incident or alert should trigger a team response? Which assets or systems, if down, would cause serious issues for the organization? What assets contain data should be monitored more closely? Understanding your landscape is critical to building an effective incidence response plan.
4. Obtain at least one board member on the incident response team including your CISO. If you cannot get the agreement to be apart, then work on that foundation and use the data at your fingertips to explain the exposure, risk and capital losses for a security incident.

5. Start with a simple incident response plan for your SOC, IR team for when a critical asset has alerts or shows signs of compromise or attack. Run simulations of this simple plan and talk about it. Tell your team why an effective and consistent response is important and get their feedback. Communication is the key to all problems.
6. Now that you have a simple plan around a key asset and a certain type of threat. Build specific incident response processes for another type of threat events. Define each of these plans around different types of threat events or attack types and take it one step at a time. Setup weekly meetings to build out a plan on a whiteboard, document, build a visual in Visio, save it, print it and build it out you IR plan book.
7. Once your IR plans or ADMIN BOOK is completed, it's time to test some of the plans. Simulations are the best way to do this. Tabletop exercises help to know what to do when something happened, who to call, how to call and when to get legal involved, etc.
8. The most important thing to remember is to train, help and work with your team. If you're not getting the cooperation from your team, the change the team, do not let the team think that a reactive, fire-fighting approach is a good approach to protecting your security posture.

Disaster Recovery Planning (DRP) can be simply defined as a document which constitutes of certain necessary and well-defined policies, procedures and action plans which would help continue operations in an organization about applications, information, technology, and other similar important resources and assets.

Figure 4 below describes the 7-Step Methodology used in the Disaster Recovery Planning in organizations. The seven steps defined are:

1. Policy Statement,
2. Business Impact Analysis,
3. Identify Preventive Controls,
4. Develop Recovery Strategies,
5. Document Disaster Recovery Plan,
6. Plan, Testing, and Training,
7. Plan and Support Material Review / Maintenance.

The above mentioned seven steps suggested that each component must be considered separately and focused on each. The steps must also be followed to reach the destination in a proper and well-formed manner. Figure 4 which represents the 7-Step Disaster Recovery Methodology gives us the best process to develop business continuity and disaster recovery plans in an organization.

Figure 4: A 7-step methodology for disaster recovery planning (Professionals, 2016)

According to Advanced Computer and Data Communications IT professionals, the primary objectives of disaster recovery planning (Professionals, 2016):

1. Minimizing the disruption of business operations,
2. Minimizing the risk of delays,
3. Ensuring a level of security,
4. Assuring reliable backup systems,
5. Aiding in the restoration of operations with speed.

They have also defined a few benefits or reasons you should consider making a disaster recovery plan that you may not have considered (Professionals, 2016):

Asset and inventory management. The first part of a good backup and recovery plan is thorough documentation, which involves understanding equipment inventory. This is useful for identifying which pieces of equipment you have, which are extra but may come in handy, and which are completely superfluous. Any good IT administrator knows which equipment he or she has and where to find it. That way if there is a problem, whether small or large, spare equipment is quickly accessible. Good asset management also helps prevent employee theft, which can certainly happen at any organization.

Network Management. How can you successfully manage a network if you do not know everything about it? Detailed documentation as part of a good backup and recovery plan helps you clearly understand the way a network is functioning, which allows you to remedy issues quickly. So, if there is a simple problem like a busted router or something awful like a server failure, you can handle it. RMM tools are great for this because they can help you document networked equipment automatically. Still, there's a physical aspect that you shouldn't ignore. Taking photos of equipment setups—particularly in server rooms or closest—can be useful as well. Oh, and don't forget the labels!

Task redundancy. Part of your disaster plan involves making sure at least two people can do any one task. This keeps you covered in an emergency, but it does not have to be a full-on disaster for task redundancy to be useful. Have you ever had somebody leave on vacation, call in sick, or leave the company abruptly and on poor terms? This can cause huge problems if that person is the only one who can do a critical task. Not only that but what about less critical tasks? As an example, suppose you need a person to perform a network diagnosis before you can fix something, but only that one person has the capability. If that person is too busy, it can create a bottleneck, and you're sitting around waiting. You could save time if only you could quickly do it yourself.

Cost savings. Here it is mentioned that good documentation could result in better management, but it can also help you identify areas where you could be saving money, particularly if it's time for a hardware upgrade. Why run three separate servers when you can run three virtual servers on one physical piece of equipment? Your eagle-eye view can help you see where the cost savings might be and where you might be able to go virtual or to the cloud.

Ability to test. How can you test a plan you don't have? If you have a disaster recovery plan, you can run through what would happen in various scenarios, which allows you to see your recovery in action. If you're an IT provider, this also helps you establish trust with clients who can watch your test and see what you can deliver on any promises you've made.

Business Continuity Planning (BCP) can be simply defined as a planning action of creating different methods to prevent systems and other resources/assets from being attacked, regarding human-errors and few controllable natural disasters (minor) and prepare backups for the same to enable easy access for business continuity and maintaining the confidentiality of information and protecting it.

Figure 5: Lifecycle of business continuity (EzeCastle, 2018)

Figure 5 shows us the general Business Continuity Lifecycle in organizations. So, the major components seen in the Business Continuity Lifecycle are Risk Assessment, Business Impact Analysis, Strategy-Plan Development, and Measure. The main phase that one can consider from Figure 5 is Business Impact Analysis.

Risk assessment. This can be referred to as estimating risk with a focus on a situation seen before or an already acknowledged threat which can be comfortably analyzed with proper results and outcomes. It can be qualitative or quantitative where qualitative would describe the description process of how one would be able to assess the risks based on previous attacks or threats. Quantitative would describe considering factors like the magnitude of loss, probability anticipation, and loss that might be detected.

Business impact analysis. This would discuss the proper procedure that one follows to find out, evaluate and analyze the after-effects in organization caused by natural disasters, human-made disasters or other similar actions. This is one of the major components of Business Continuity Planning.

Strategy and plan development. Here the main phases of business continuity is how to design and develop a proper business continuity and disaster recovery plan. Here one would need to activate proper strategies and create well-formed plans to create good disaster management approaches.

Measure. This refers to the training, testing, and maintenance phase. Training is a must phase where professionals should know about what plans are made to act accordingly during the time of disasters or incidents. Testing and Maintenance are also the important phases where the plan needs to be updated and checked at regular intervals whether the plan is working according to our expectations.

There are different business continuity plans followed by different organizations. Let us have a look at two examples below. This plan was proposed by Kim and Ed, which says (Tittel, 2017):

1. Identify the scope of the plan.
2. Identify key business areas.
3. Identify critical functions.
4. Identify dependencies between various business areas and functions.
5. Determine acceptable downtime for each critical function.
6. Create a plan to maintain operations.

The above-developed plan looks good but quite simply which can be used in small-scale organizations. Now let’s see another example defined by Investopedia Professionals (Investopedia, 2018):

1. Conduct a business impact analysis to identify time-sensitive or critical business functions and processes and the resources that support them.

2. Identify, document, and implement to recover critical business functions and processes.
3. Organize a business continuity team and compile a business continuity plan to manage a business disruption.
4. Conduct training for the business continuity team and testing and exercises to evaluate recovery strategies and the plan.

Literature Related to the Problem

Kenya is one of the countries from the Africa continent, and one can see that in today's era, Kenya has developed good towards Information, Communication, and Technology (ICT) and produce well-formed services to the customers and users. With this quick development in Kenya in terms of technology, businesses, and communications one can see that Parastatals and other organizations will have threats and risks from internal/external disruptions or attacks as information has moved up in terms of size and quality. 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 the cost of business as well as reducing the cost of communication, management, and transaction of data (Nalo, 2007).

According to a 2006 Handbook for Civil Service Staff induction, a Parastatal is a state corporation or agency mainly established by a state or an Act of Parliament in pursuance of Government policy. Parastatals can be defined as ministries that have links with the Central Government and work with them side-by-side with respective government sections of operation. Here there are divisions in parastatals which depends on respective revenue base, size of the

asset and the ministry under which the parastatal would be part of. For example, one can give the following as examples of Parastatals:

Kenya Revenue Authority (Financial Sector)

Kenya Pipeline Co

Kenya Power & Lighting Co

Electricity Regulatory Board

Kenya Agricultural Research Institute (Training and Research Institution Sector)

Higher Education Loans Board (Service Corporation)

Why Kenya? Kenya is one of the major countries in the African continent and serves as a founding member of the East African Community (EAC). Though Kenya is one of the big and advanced cities around Africa, it is still behind on the Human Development Index, and the economy of the country is very poor. But now one can see how good the development is happening in Kenya regarding tourism, education system, telecommunications sector and agriculture where one sees quite as the vital tea sector is doing well. Literacy percentage here is low as one sees much of child labor and prostitution is encouraged here and hence the education system is not so good. Education leads to better development of knowledge and helps to develop and create new things and try to bring up the economy of the country. Kenya is also very much prone to both natural disasters and human errors or human-made disasters like software failures and hardware failures.

Table 2

Droughts and Their Effects in Kenya (Huho, 2016)

Year	Disaster type	Area of Occurrence	Effects
2012	Drought	Widespread	3.75 million people in dire of food by July 2012
2011	Drought	Garissa, Isiolo, Wajir, Mandera, Mombasa, Marsabit, Nairobi, Turkana, Samburu and Turkana Counties	4.3 millionpeople were in dire need of food
2009	Drought	Widespread	70-90% loss of livestock by Maasai pastoralists
2007-08	Drought	widespread	4.4 million people affected, 2.6 million people at risk of starvation, up to 70% loss of livestock in some pastoral communities.
2006	Drought	Widespread	3.5 million in need food by September.
2005	Drought	Widespread	40 human lives lost and about 40% cattle, 27% sheep and 17% goats lost 2.5 million people close to starvation. Declared a national disaster
2004	Drought	Widespread	About 3 million people in need of relief aid for 8 months to March 2005 70% loss of livestock in some pastoral communities
1999-2001	Drought	Widespread	4.4 million people affected

Table 2 above discusses the droughts that have made huge impacts on Kenya almost every year. The impact leads to the loss of lives and the loss of livestock. This shows how much Kenya prone to droughts is. If you look at the latest statistics, i.e., during the year of 2012, one can see that there was a loss caused to about 3.75 million people in terms of food and health since the drought was almost widespread around a large area.

Table 3

Road Accidents and Their Effects in Kenya (Part-1) (Huho, 2016)

Date/ Year	Type of accident	Where	Deaths	Injured
Jan 7, 1998	Bus plunges into Nithi River	Meru	58	42
Mar 29, 2000	Two buses collide	Kericho	74	
Nov 7, 2000	Bus flew over a bridge	Meru	45	35
Aug 15, 2001	Minibus plunges into Mwania River	Machakos	23	
Apr 14, 2007	Matatu overturns and bursts into flames	Garissa	15	61

Table 4

Road Accidents and Their Effects in Kenya (Part-2) (Huho, 2016)

Date/ Year	Type of accident	Where	Deaths	Injured
Feb 4, 2012	Two mini buses collide	Kisumu-Kakamega highway	26	
2012	Bodaboda accidents	Countrywide	415	1,984
Aug 29, 2013	Bus accident	Ntulele, Narok	42	44
Dec 24, 2013	Collision of two buses	MtitoAndei	18	67

Table 3 and Table 4 shows us the statistics on road accidents that happened in Kenya. If one considers an average number of deaths and injured people in every road accident, one can judge that there were about 20 deaths and about 30 injured cases on an average which is quite high in terms of lives. This can mean that the condition of roads and vehicles are not in proper and well-formed. This must be bringing an approach towards development on the transportation side to save the lives of people.

Table 5

Floods, Landslides and Their Effects in Kenya (Huho, 2016)

Year	Disaster Type	Where	Effects
2015	Floods	Widespread	15 people killed and thousands displaced Infrastructure destroyed
2014	Floods	Narok Town, Nairobi City	Property and infrastructure destroyed
	Landslides	Muranga County	
2013	Floods	Tana River County	82,000 people displaced
	Landslides	Nyeri, Murang'a, Kisii	2000 people displaced
2012	Floods	Nyanza/Western	84 people killed, 30,000 displaced About 280,000 people affected countrywide
	Landslides	ElgeyoMarakwet County	10 people killed, hundred displaced
2010	Floods	Budalangi, Tana river, Turkana	73 killed, 14,585 people affected
	Landslides	Bududa,Mt Elgon ,Samburu	3000 people buried, property destroyed
2008	Floods	Rift valley, Kitale, Makueni, Mwala/Kibwezi, Bundalangi	24 people killedwith 2396 affected
	Mudslides	Pokot central	11 people killed
2007	Mudslides	TaitaTaveta County	3 dead

Table 5 discusses the floods and landslides that have occurred in Kenya. Based on the above statistics, it shows us that some major floods and landslides have occurred almost once in every year and made a huge impact at the cost of a large number of lives. These natural disasters cannot be controlled by humans, but preparations and plans can be developed and deployed to save lives shortly.

Table 6

Terrorism Activities and Their Effects in Kenya (Huho, 2016)

Date/ year	Nature of the attack	Causalities
Aug 7, 1998	Al-Qaida terrorists attack U.S. embassy in Nairobi	15
Nov 28, 2002	Terror attack on Israel owned Paradise Hotel in Kikambala, Mombasa	None
Nov 28, 2002	Terrorists fired a missile at an Israeli Arkia Airlines jet but missed their target	None
Oct 24, 2011	Al-Shabaab launches a series of low-grade terrorist strikes in Nairobi	2
Oct 24, 2011	Attackers hurl grenade at a commuter bus stage in Nairobi	1
Oct 27, 2011	Al-Shabaab militants attack a vehicle transporting examination material in Lafey, Mandera	4
Nov 5, 2011	Two grenades hurled at the East African Pentecostal Church in Garissa town	2
Nov 24, 2011	Twin grenades attacks at Holiday Inn hotel and a shop in Garissa	3
Jan 11, 2012	Suspected Al-Shabaab militants kill six people in Gerille camp, Wajir District and kidnapped two government officials.	6
Mar 10, 2012	Four hand grenades hurled at Machakos bus station in Nairobi	6
July 1, 2012	Twin church attacks in Garissa town	17
Sep 21, 2013	Armed gunmen attacked the Westgate Shopping Mall in Nairobi	69
June 16, 2014	Suspected Al-Shabaab militants launched a major assault on a police station, hotels and government offices in Kenyan coast	48
Nov, 22 2014	Gunmen attacked a bus traveling from Mandera to Nairobi	28
Dec 2, 2014	Suspected Al-Shabaab militants attacked and killed a further 36 quarry workers	36
June 15, 2014	Suspected Al-Shabaab militia attack Mpeketoni village in Lamu County	50
April 2, 2015	Suspected Al-Shabaab militants attacked Garissa University College	147

Seeing natural disasters making huge impacts in Kenya was not enough. From Table 6, there are human-made incidents which have also been a part of making huge impacts where terrorist activities were so active that one can see that there were on an average about three incidents happening every year. This means that Kenya has been a target to a huge group of terrorist activities which have taken control of Kenya for a short time and impacted quite several casualties.

Problems in Implementing a Business Continuity and Disaster Recovery Plan in Government/Parastatals

From the above-discussed tables, one can infer to what level, Kenya has been prone to various kinds of disasters both in terms of natural and human-made/human errors. 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 (Juniper, 2009).

There were some general challenges seen with the implementation of traditional disaster recovery as discussed below (Valent, 2016):

On May 21, 2015, OnRamp Founder Chad Kissinger and GCS Technologies President Joe Gleinser took part in a panel discussion titled “Disaster Recovery–Surprising Challenges.” Mr. Gleinser identified the following points as one of the important challenges faced (Valent, 2016),

1. Making the Formation of BC/DR Plan as a Business Priority.
2. Ensuring the Completeness of Planning.
3. Going it alone.

From the above challenges, one can know that Business Continuity and Disaster Recovery Planning has not been an important component in organizations because they feel that it is not needed today or tomorrow just like insurance coverages. But whenever an unexpected event is bound to happen, the situation is never in control of ours since there was no pre-planning about how to act after the event. So, it’s always best to see BC/DR planning as the first or equal priority in comparison to other software functions, infrastructure design, and staffing.

In other organizations, one sees that there is BC/DR planning done but is left incomplete. To complete a BC/DR planning the general five steps defined by security and disaster-related professionals are:

1. Development;
2. Implementation;
3. Testing;
4. Evaluation;
5. Maintenance.

The general meaning of the above five steps is to be up to date with a link to the latest developments, security algorithms/techniques and large data handling in software organizations. This would thus let us know that development would need a strong analysis of the different processes in an organization and then implement proper backup and recovery plans. Here one must then test the plans at regular intervals to make sure it is coordinating with the changes happening in an organization every year or every month. The final step is to maintain the BC/DR plan to ensure data is up to date and regular checking must be done on the plan created and see if any changes in the plan can be made to make sure everything is in place.

Another factor is that one can see that a good number of organizations have the idea of sharing BC/DR plans to ensure help to each other during the times of crisis. But every organization is different from each other. So, one needs to make sure that every organization has its own BC/DR planning since they can concentrate on the actual assets and resources of the respective organization.

Summary

In today's era, one can see that there are a group of types of disasters happening around the world and in which Kenya has been prone to many types of attacks from the human-made level to the natural level. The government agencies and organizations here have completely ignored business continuity and disaster recovery planning due to various factors such as cost, increase in human effort and complexities in a few methods. Here are discussed the types of disasters Kenya has faced and has included about the three terms to be focused by the organizations which are Incident Response, Disaster Recovery and Business Continuity and about what state is the planning done in Kenyan organization and parastatals.

Chapter 3: Methodology

Introduction

This section would give us an idea of how we would be proceeding with our study about the disaster management conditions in Class A parastatals. We will here see about the state of disaster management planning in Class A parastatals based on a previous survey and then collect enough information to analyze the benefits and challenges involved with business continuity and disaster recovery planning. One would see what data will be useful to us and how the sample size of the previous survey would determine our analysis. This chapter would thus introduce our methodology of how one would reach our destination of this study depending on various resources we use in here.

Design of the Study

The design here would be having in our study is both qualitative and quantitative. We first analyze the survey done around 18 parastatals where a set of questionnaires were used to analyze the situation of the extent to which the disaster management has been focused on and how protected are the assets and data in parastatals. We would then refer to techniques with cost and maintenance in mind and explain how useful these cost-effective methods can be to plan disaster management and how to bring up awareness towards educating people about disaster management and help to be ready at the time of disaster which can be either human-made or natural.

With the use of the survey done in Kenya by the employees of parastatals, one can infer few details from that regarding the benefits (If any) and challenges that are found in the BC and DR plans which are already created and whether they are tested and maintained at regular intervals. Based on all the factors one would be providing recommendations, technologies or

software and awareness to educate people about how to act on when any attacks happen in parastatals and organizations or institutions.

Examples from other countries would be considered in our research study which would help us in bringing up a strategy for building a business continuity and disaster recovery plan. Above mentioned research questions would be taken into consideration while processing our analysis. Several research resources would be explored for developing effective business continuity and disaster recovery strategies that can be implemented for the state organizations (Parastatals) in Kenya with their resources, economy, and information in mind.

Data Collection

Here would be collecting data from the previous survey and analyze them based on the current situation of the BC/DR plans in Class A parastatals and ensure proper and cost-effective plans so that the Class B and Class C parastatals can follow the same. In here a collection of other information will be from academic articles, on-site (web) certified journals, IEEE papers, well-written whitepapers, academic books and other documents from the website. Here, mainly there will be using the internet as our main source for our study because many organization will not be in a state to provide us with details regarding their strategies as they are confidential information. We would be focusing on the various latest technologies and cloud services where the cost will not be a concern and will be an effective way for BC/DR planning. The research questions stated would be kept in mind and answered at the end of our study.

Research Questions

Chapter 1 lists a few research questions in which planning for data analysis will be done. As mentioned before, a previously-done survey would be one of the main sources in our research study. The following research questions would be analyzed and answered accordingly.

1. What are the business continuity and disaster mechanisms developed by Class A parastatals in Kenya?

   For the above questions, there would be an analysis of the current state of Kenya State Organizations in their implementation and education about business continuity and disaster recovery. The present situation there would be analyzed, and the drawbacks will be collected for our research study.

2. How is awareness about Disaster Management brought in at educational institutions and government/private organizations of Kenya?

   Here there would be a study about how the people in Kenya are provided with education and training about the disaster management and what actions have they planned for during any disasters happening around them and how they would protect resources, assets, people and information.

3. What practices are used to create and implement business continuity and disaster recovery plans in Kenya? How would the plan be reliable and maintained, and how cost-effective the plan could be with dependencies over the resources and budget provided for the state organizations in Kenya?

   Analysis from the previously-done survey would help in giving us some information about what factors are the main concerns in organizations. Considering the factors, implementation would be created based on examples and technologies from other countries and see how their mechanisms can be used differently in Kenya. Here have considered a few important things from developed countries and try applying them to the Kenya State Organizations based on their resources, budget, and information to handle.

Other Sources

As told earlier, based on our analysis from the survey, we would be providing recommendations about various cost-effective and easily-handled methodologies of how to prepare the Class A parastatals against any attack or disaster and how quick would they be able to continue their operations and functions without any much disturbances and help the lower-class parastatals in their strategies. Education about disaster management has to be improvised, and we would be proposing how to create awareness among the people of Kenya to focus on disaster management to protect their assets and resources.

A previously-done survey would help us in the analysis of the present situation of the business continuity and disaster recovery planning. We would be collecting as much information as possible and provide the proper use of technologies, software applications and cloud services used to prepare Class A parastatals from attacks as they constitute large data which cannot be compromised. One would also see to what extent are the people educated about disaster management and then provide them awareness solutions and most importantly focus on the check at regular intervals.

This study would thus be focusing on the Class A parastatals of Kenya and based on the survey results; one would be considering different factors which would be used to help us identify which areas to concentrate on while preparing BC/DR plans. These methods or technologies will be not only helpful in Kenya but also in other organization around the world which would be brought down the time-consumption to recover, cost, workforce, and other related factors.

Summary

This chapter gives us a basic idea about how the study would be done about the business continuity and disaster recovery planning for Kenya State Organizations. This chapter discusses how the study would be done in a proper procedure like what sources will be used, qualitative or quantitative, the timeline for completion of our study, etc. All the sources and data will help in developing proper business continuity and disaster recovery strategies. Class A parastatals are one of the main concerns that have been chosen because of the many government ministries with huge revenue and information it consists of.

Data Analysis

In this study, a survey is taken under consideration which was conducted by one of the Kenyan students in their country using government officials as the objects to answer his questionnaires. The government officials involved in this survey have given in their knowledge and feedback regarding various information related to disaster management as to how and to what extent are, they educated and trained towards emergency and natural disaster situations. This data collected from one of the surveys is going to be one of our important aspects in our research methodology where we try to filter out the things that are known to them and identify areas where they have not any knowledge or information about. One can extract as much information required from the analysis below on the disaster recovery and business continuity plans present in the Class A parastatals or official government offices.

According to the survey information, one can see that 54 people that are related to government functioning have been involved in this survey which consists of both males and females. Here one can see that there is almost an equality on the percentage of men and women who have involved in this survey which is a good sign that we have had views or reviews from

both the male and female perspective. As you see in the below pie chart, it shows us the percentage of men and women that have been involved in completing the questionnaire as required by the survey requirements. There were personal arrangements and on-call reviews done to complete the survey as per the period.

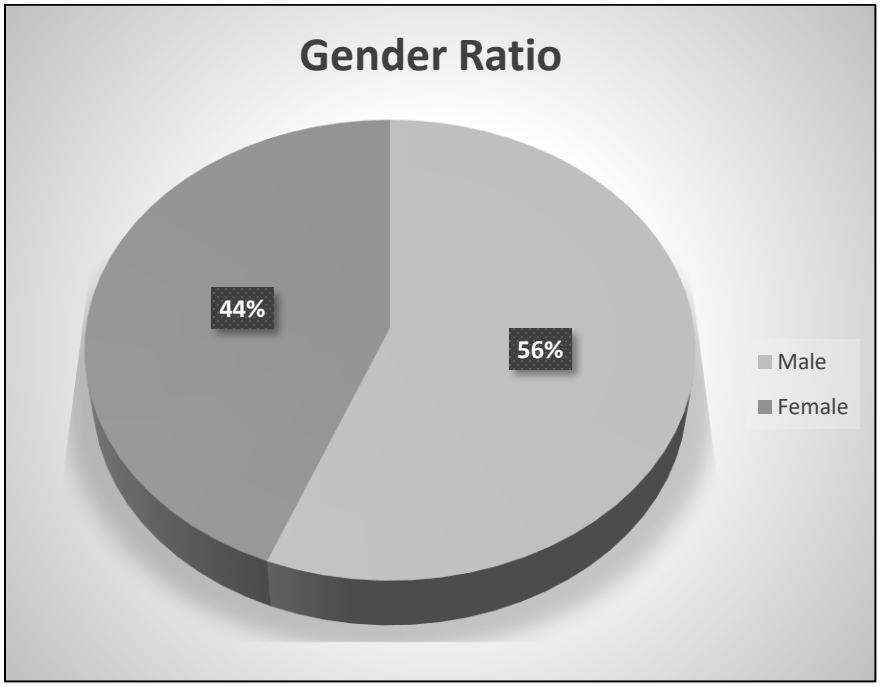

Figure 6: Gender ratio (Mathenge, 2011)

From the below pie chart, one can also infer regarding the age of the official government people involved in this survey. Now from the below picture, one can see that

1. Age 21-30: 26%;
2. Age 31-40: 50%;
3. Age 41-50: 24%.

The above information suggests that there is a good quantity of youth and middle-aged people involved working for the government which is a good sign on the future of the students

studying there back in Kenya. It's a good thing to know that Kenya is always supportive of education and employment.

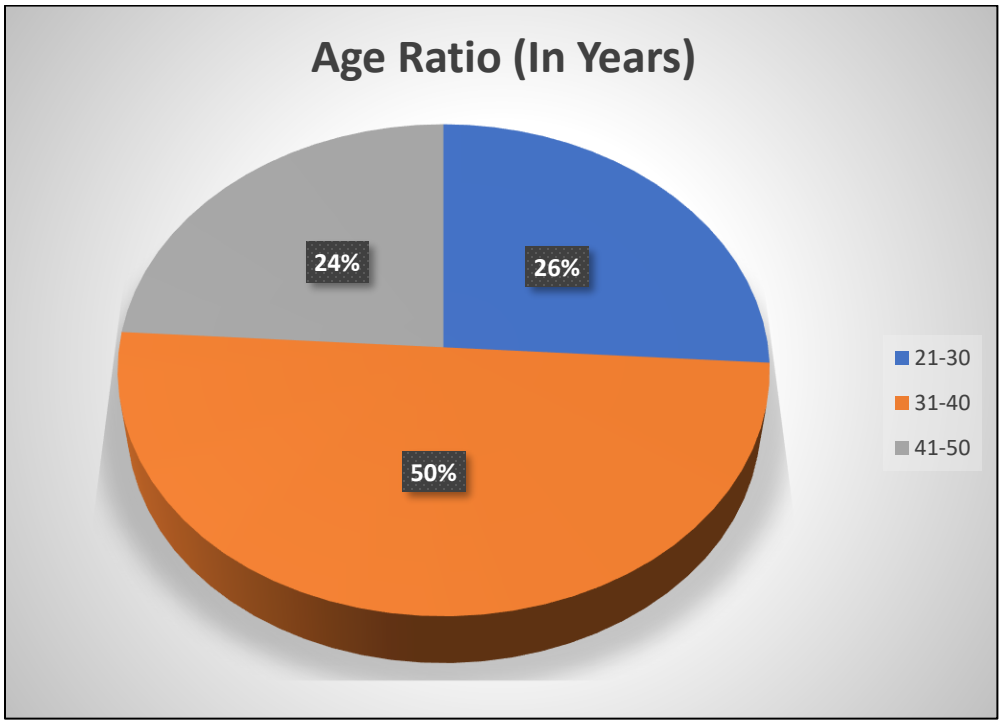

Figure 7: Age ratio (Mathenge, 2011)

Now approaching the education levels that are observed for the government people who have involved in this survey is shown below:

1. 22% - College degree;
2. 70% - Graduate degree;
3. 7% - Post-Graduate degree.

Now 70% of people holding a graduate degree is another good sign, and this must be really good statistics on the number of people who are pushing themselves towards education and earning a high-level degree.

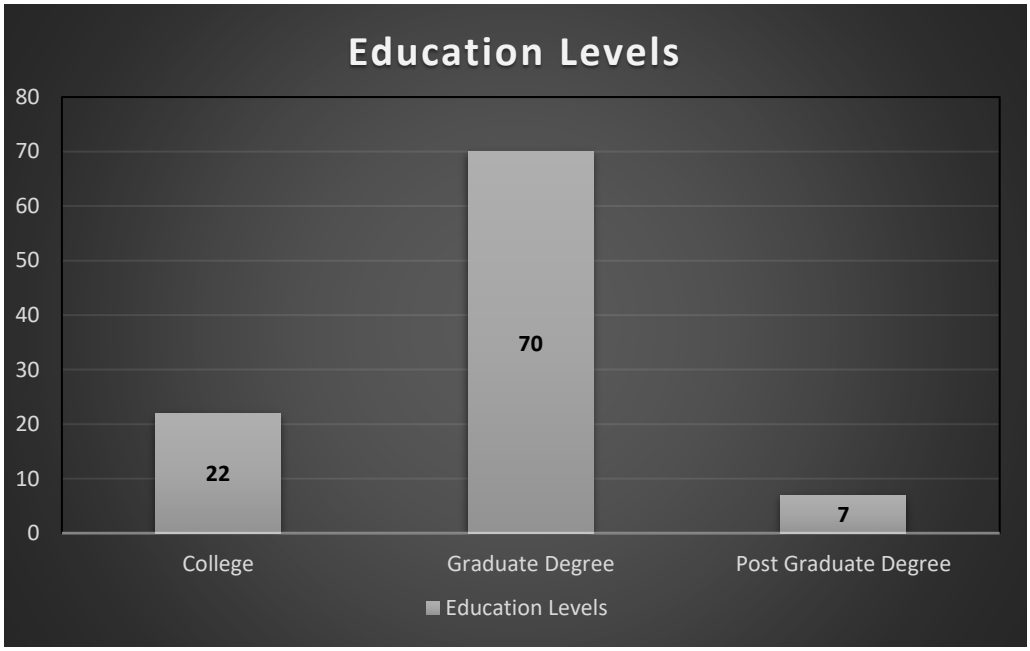

Figure 8: Education levels (Mathenge, 2011)

From the above three figures, one can see how old and how educated the people are who have involved in this survey conducted in Kenya. Since this is an important aspect on the information required on disaster recovery and business continuity, one can see that well-educated and experienced government people have been involved in giving us some good knowledge and information about the planning and execution phases of disaster management at government offices.

Table 7

Pre-Planning Phase (Mathenge, 2011)

RANK	Preplanning Phase (Acceptance Criteria Levels)	Small Scale	Medium Scale	Large Scale
1	Consult business process owners during the BIA.	28	21	52
2	Prioritizing business process by performing BIA (Business Impact Analysis)	23	26	51
3	METHODOLOGY - Industry Standard Disaster Recovery (DR)	31	44	25
4	Preparation of a recovery options list that itemizes recovery options by business processes.	60	23	16

The points mentioned above are one of the important factors to be considered during the Pre-planning phase where it all discusses the actual steps to be considered before preparing a disaster recovery plan or a business continuity procedure. The main factor that was identified by most government workers was consulting the business process owners during the BIA. BIA refers to Business Impact Analysis which is a statistical procedure to evaluate certain factors based on the respective expected/unexpected impacts that could be occurring at any time all over the year. As an example, consider the following factors that can be considered as objectives of a Business Impact Analysis are (Taylor, 2013):

1. Identify all business functions within each department of functioning in the respective organization.
2. Assigning each function, a Recovery Time Objective and provide justifications for the same.
3. Identify the applications that are supporting business functions.

4. I am assigning the application criticality which is based upon their respective business functions.
5. It is identifying upstream and downstream dependencies that may affect the delivery of goods and services.

The information mentioned above is an example of how to approach preparing a Business Impact Analysis. Accordingly, one can observe that most of them in the survey have accepted towards their knowledge on consulting the business process owners for BIA (52%) and performing a BIA to prioritize your business process (51%). There has been a very low percentage observed on the factor about the preparation of a recovery options list that itemizes recovery options by business processes (60%-Small Extent). It is always better to have a checklist on the recovery options which eases us to prepare quick recovery processes accordingly. Every business has different items to prioritize on. So, preparing a checklist on recovery options is always helpful. And then here the below average responses on the other factors of Industry Disaster Recovery Methodology (44%-moderate extent) and performing risk management reviews to identify and correct obvious weaknesses (44%-moderate extent). Based on the above information, things look good, but there is still quite much room for improvement when compared to the Business Impact Analysis. Other factors need to be taken care of and must always be prioritized.

After the Pre-planning phase, here comes the Planning phase which is the most important phase where people really must have good knowledge and be trained upon. The below table shows us some information on this phase and its feedback.

Table 8

During the Development Phase of a DR and BC Plan (Mathenge, 2011)

Rank	Development Phase (DR and BC Plan) - Acceptance Criteria Levels	Small Scale	Medium Scale	Large Scale
1	Designate a location of backup tapes	6	14	79
2	Document emergency response procedures to occur during and after an emergency	7	16	75
3	Formal system backup policy and schedule	12	15	73
4	Inventory of assets needed for offsite recovery (example: backup tapes, operating system software, etc.)	17	22	61
5	Define a call tree for notifying your staff when a disaster is declared	7	38	53
6	List of detailed tasks needed for offsite recovery	7	38	53
7	Measures to manage contingency processes while your IT systems are being recovered	16	28	53
8	Investigate new advanced technologies that can reduce downtime	25	22	53
9	Develop a disaster organization chart that defines recovery teams	27	22	51
10	Develop a key vendor contact list	33	23	39
11	Consideration has been given to developing the BC plan around a worst-case scenario	42	23	31
12	Understand the company time and data requirements (e.g., how much downtime can the company afford)	55	25	19
13	Vendors' approval for their inclusion in your plan (e.g., will they be available, under contract, etc.)	65	19	16
14	Appoint a public relations team to address external inquiries	89	8	3

The above information produced infers that their great extent of knowledge upon designation of a location for backup tapes (79%-large extent) and document emergency response procedures to occur during and after an emergency (75%-large extent). Designation of location for backup tapes is now an outdated approach towards protection and saving the information or data. In today's era, one can see how far the technologies have reached which can allow us to store data over the internet now safely and securely without any much efforts. This means that the government offices have been maintaining their information and other important stuff in an old-fashioned and formal methodology. They should now be open to the new stuff where technology is involved, and there is no need for any physical locations to store your backups. An example of better backups is as given below which has been a standard in Fujitsu and can be inherited from (Fujitsu, n.d.):

1. Use smarter passwords.
2. Use Biometrics or even smarter things than passwords.
3. Back up on data and eradicate data on used drives.
4. Stop thieves getting a hold on your data.
5. Stay up to date and keep on patching.
6. Lock devices up.
7. Protect encryption keys.
8. Encrypt the whole drive.
9. Manage security on user-owned devices.
10. Identify vulnerabilities and create your action plan.

The above example gives us some simple and easy features that can be inherited and used at the government offices in Kenya. This would need some training and education towards the

smart computers and its smart options which can help store data, access data securely and work safely without any discrepancies. So basically, one makes sure to protect their data both physically and digitally at once using the smart ways. From the table, one can also observe that the formal backup procedure and schedule is the third-ranked and most agreed factor by various government people involved in this survey (73%-large extent).

When one considers the other leftover factors, there's not much percentage accepting to the information where external vendors were not contacted to help out, investigation on new advanced technologies which can reduce their runtime (53%-large extent), consideration has been given to a Business Continuity in a worse-case scenario (31%-large extent) and understanding on company time and data requirements (19%-large extent).

One must always consider a worst-case scenario which can make people educated and prepared of about how to react during times of emergencies especially when the impact is high. To get a better understanding of that, one must learn about the various aspects of their respective companies and look for the best solutions that can be investigated during the time of an emergency. The planning phase section looks outdated and has room for much to fit in. Especially the software side can always be enhanced and developed by educating and training people at high priorities with advanced technologies and executing them in the government offices and other private organizations.

Table 9

Testing Phase of a DR and BC Plan (Mathenge, 2011)

Rank	Testing-Phase (Acceptance Criteria Levels)	Small Scale	Medium Scale	Large Scale
1	Frequently scheduled tests	7	16	75
2	Development of a test plan	12	21	66
3	The formal process to certify the success of your testing, e.g., Test results documentation	14	19	66
4	Establishment of testing success indicators in the test plan	16	21	62
5	Testing of remote office connectivity as a success indicator	16	21	62
6	Total time for execution of recovery tasks as a success indicator	28	21	52
7	Testing of restored systems as a success indicator	28	21	52
8	Use of incidents as a form of testing	22	44	32
9	Independent observer to validate the test results	58	12	31
10	Segmentation of overall plan into sections that are easily tested.	52	33	13

After the planning phase, comes in the plan testing phase, where one must see if everything is going well with our preparation phase. The plan we develop must always be tested through before it is turned in for execution during an emergency or disaster-related human-made or natural calamities. The Business Continuity and Disaster Recovery plans are first planned for how it should like and then the testing phase in brought into action. The testing phase should be made sure that it is updated and reviewed at regular intervals throughout the year to get people aware of the steps to follow during emergencies.

In this phase, the factors such as frequently scheduled tests (75%-large extent), development of a test plan (66%-large extent) and formal processes to certify the success of testing (66%-large extent) has been accepted by quite many which is a good sign towards a business continuity and disaster recovery approach. Formal processes to certify the success of testing sounds to be an outdated process, but one can also have many technologies which can automate the testing phase at regular intervals and better help during emergencies without much physical efforts from people. This kind of testing is always suggested and supportive because many government offices have important and confidential data that must be protected and stored safely. The advanced technologies can always be helpful in the testing phase where people would not have to put in manpower and rather use mental power to speed up the recovery process during times of emergency.

The Disaster Recovery and Business Continuity Plan Testing phase are to ensure the following as identified by one of the authors from the SANS Institute (Martin, 2002):

1. Simulate the conditions of an ACTUAL Disaster Recovery situation.
2. Completeness of the disaster recovery information stored at the Records Retention Site.
3. Ensure the ability to recover the intended functions.

They have also discussed the different factors or areas that the business continuity and disaster recovery testing phase would include. This consists of two sub-areas namely Pre-Test and Post-Test (Martin, 2002):

Pre-Test

1. Schedule
    a. Planning Sessions
    b. Pre-Test Technical Review
    c. Debriefing
2. Introduction
    a. Preface
    b. Scope
    c. Recovery Site
    d. Primary Test Objectives
    e. Secondary Test Objectives
    f. Exclusion (if applicable)
    g. Test assumptions, dependencies and success criteria
3. Test Teams
    a. ChoicePoint Participants
    b. IBM Participants (if applicable)
4. Pre-Test Planning
    a. Activities
    b. Issues
    c. Concerns
5. Test Timeline
    a. Planned start and stop time and tasks.
    b. Actual start and stop time of tests and tasks.

6. Critical Test Checkpoints
    a. Activity
    b. Recommendation
    c. Responsible party
7. Test Problem Log
    a. Document any problems encountered before the test.
    b. Record any deviations from the test plan.

Post-Test

1. Highlights
    a. Overall Test Results
    b. Test Dates
    c. Disaster Recovery Backup Site
    d. Local Access Suite
    e. Test Participants
2. Test Objectives
    a. Primary Test Objectives
    b. Secondary Test Objectives
    c. Exclusions (if applicable)
3. Timeline
    a. The planned task, start and end times and duration
    b. Actual start, task and end times
4. Problems encountered during the Test
    a. Problem Log

- Actual Problem
- Assigned to
- The target date for resolution
- Status
- Resolution
- DR Process or Technical

b. Problem Summary

5. Follow up to Pre-Test problems.
6. Follow up to Suggestions for Improvement/Recommendations from Last Year's test.
7. Detailed Summary and Observations.
8. Recommendations for the Next Year's test.

The two phases of Pre-test and Post-test as discussed above by one of the authors from SANS Institute can be very helpful during this plan testing phase where one can easily prepare documentation considering the example and identify risks and its solutions accordingly.

Segmentation of overall plan into sections that are easily tested (13%-large extent) is the least accepted factor in this survey. Dividing the work into small modules is always a better plan which would make things easier. As the example discusses the various steps, one can see how huge the procedure seems to be. If those steps can be divided into sections and assigned to specific people on specific sections, then one would have a better testing phase, and the process can be fastened. Independent observed to validate the test results (31%-large extent) is also one another less accepted factor and should be investigated. A few people can be assigned to keep observing during the test phases which helps in proper monitoring of the test phase. This testing phase has to be executed properly, on the whole, to observe good results and identify the

positives and negatives from it. Disaster recovery testing shows you your weak points or places where your data is vulnerable to lose or corruption (Baseline, 2015). This completes the plan testing phase which has given us enough information and examples of how to test any plan to use it.

Table 10

Maintenance Phase of DR and BC Plan (Mathenge, 2011)

Rank	**Maintenance Phase for a DR and BC Plan (Acceptance Criteria Levels)**	**Small Scale**	**Medium Scale**	**Large Scale**
1	Provide a mechanism for regular review and evaluation on a predetermined schedule	7	16	75
2	Establish agreements with critical vendor and service provider	12	15	73
3	The formal process for maintenance as your environment changes	12	21	66
4	Have an existing change management system to automatically update the DR plan	8	32	59

After the Plan Testing phase, here one sees the Plan Maintenance phase. This is one of the important aspects of our disaster recovery and business continuity planning since it must be made sure that the things in the plan must be updated or upgraded accordingly and maintained the same. From the above table, providing a mechanism for regular review and evaluation on a predetermined schedule has been one of the most accepted factors and is true. There should always be a predetermined schedule which should support the plan maintenance section. A few things must be considered well in advance to make the review on the plan better. A team can be formed in here who will be concentrating mostly on the plan maintenance phase and make sure

that things are in order without any disturbances. They can themselves create some automated mechanisms for a regular review or evaluation of the plan implementations.

According to the factors mentioned in the plan maintenance phase, all the rest of them were quite acceptable in the survey. The other factors considered there are formal processes for maintenance as your environment changes, having an existing change management system to automatically update the Disaster Recovery (DR) plan and establishing agreements with critical vendors and service providers. The advancement of technology and software around should be one to be focused on easing processes on the Plan Maintenance phase. The maintenance and engineering personnel can always provide important input on utility and infrastructure improvements that can mitigate crises, improve resiliency, and eliminate points of failure (Voorde, 2014). This means that dividing a separate team for the plan maintenance phase can always be helpful and useful where they can investigate further issues or discrepancies observed in the plan implementations.

From the above information observed and discussed where it is seen that the four main phases that are used in disaster recovery and business continuity planning:

1. Pre-Planning Phase;
2. Plan Development Phase;
3. Plan Testing phase;
4. Plan Maintenance Phase.

The positives and negatives have been observed in the four phases based on the functioning of government parastatals (offices) in Kenya and need some tuning in their disaster management planning and execution mechanism.

Table 11

Benefits of a DR and BC Plan (Mathenge, 2011)

Number	**To what extent are the following considered as benefits of a DR and BC Plan**	**Small Extent**	**Moderate extent**	**Large Extent**
1	Competitive Edge	90	10	0
2	Reduction of Insurance Premiums	50	45	5
3	Improved understanding of the business is gained	10	18	82
4	Legal Compliance	37	55	8
5	Reduced inefficiencies	6	15	81
6	Reduced bureaucracy	88	2	10
7	Better Communication	40	37	23
8	Increase Value of Business	16	4	80
9	Risk Reduction	2	12	86
10	Increased customer confidence	71	23	6
11	Increased employee loyalty as their livelihoods are protected	69	22	9
12	BCM helped simplify complex processes	4	6	80
13	Reduced Downtime	10	12	88
14	Safeguard of Shareholder value	3	23	74
15	Minimize financial losses	2	32	66

After the four phases discussed in the above sections, the benefits of implementing disaster recovery and business continuity plan need to be studied. The above table describes the various benefits of implementing a disaster management activity. The main benefits or advantages observed by the people involved in this survey are Reduced Downtime and Risk Reduction. This is a good indication of benefits observed which does not cause any discrepancies in the business processes, and there's a protection to information, people and assets. Creating a disaster recovery and business continuity is hence always a positive move towards the success of an organization.

There are many advantages when disaster recovery and business continuity plan as described below (Venclova & Vydrova, 2013):

1. Long-term experience in the application of disaster recovery planning and business continuity mechanisms. (time criterion)
2. Assurance of rapid recovery of normal operating functions. (time criterion)
3. The competitive advantage is given by response to crises and preservation of critical knowledge in the organization. (financial criterion)
4. The possibility of mutual benefit in using existing standards. (space criterion)
5. Specific Business Continuity Mechanisms and Disaster Recovery Plans for each organization in each sector. (structural criterion)
6. Retention of critical knowledge and key employees in the organization. (Human Resource criterion)
7. National support for new skills and knowledge. (Government criterion)
8. The company appreciates and motivates specialists in this field of Disaster Recovery and Business Continuity operations. (Government criterion)

The above advantages describe how efficient things are when focusing on disaster recovery and business continuity. The company grows, the knowledge grows, the people grow, and overall this all contributes towards the success.

The other strong factors that play an important role in the benefits of implementing disaster recovery and business continuity plan are improved understanding of the business is gained, reduced inefficiencies, Business Continuity Mechanisms helped simplify complex processes and increase in the value of the business. Since there is reduced downtime, business always expands and grows as there is no discrepancies or disturbances observed due to

downtime. The pre-planning, plan development, plan testing and plan maintenance phases contribute towards the success of the reduced risk factor in the benefits section. Reduced risk is always a strong point since the company or organization would be well-prepared in advance to face any kind of threat or disturbances that may or can occur in the organization. Introducing the concept of Business Continuity Mechanism has always been helpful. Without this kind of mechanism, the organization would be looking at formal and traditional time-consuming methods for the planning. Business Continuity Mechanisms has played one of the significant roles in dealing with complex issues and getting out the best results contributing to reduced downtime. Looking at the four phases of pre-planning, plan development, plan testing and plan maintenance, there should be a better studying on the functions and structure of an organization or a company which means that this leads to a better understanding on business from a worker point of view. Massive knowledge can be gained during this period of looking at every nook and corner of the business for information, data, assets and other related stuff. A better understanding of business can also lead to better developments and enhancement of creativity in the organization. Minimizing financial losses is also another important factor to be considered because it is rather better to spend some time and money on disaster recovery and business continuity than to lose money on the ongoing business processes after an act of an emergency. Always better to be well-prepared in advance and minimize the loss to the greatest extent.

Table 12

Challenges Observed while Implementing DR and BC Plan (Mathenge, 2011)

Rank	Challenges of implementing Disaster Recovery and Business Continuity Plan	Small Scale	Medium Scale	Large Scale
1	Procurement delays	8	8	85
2	Bureaucracy	7	15	78
3	Identification of right stakeholders	16	8	77
4	Business reengineering challenges	16	23	61
5	Delay in payments	12	29	59
6	Lack of senior management support	31	19	50
7	The difference in Work Culture Change	31	23	46
8	Incomplete requirements	16	45	39
9	Conflict of interest in influential project stakeholders	27	42	30
10	Poor supervisory	50	35	16
11	Corruption	77	18	5
12	Government Interference	96	3	2
13	Challenges of Project Sponsor	84	16	0
14	Change of Government	100	0	0

The above table discusses the various challenges during the implementation of disaster recovery and business continuity plan. The most identified challenges in our survey are procurement delays (85%-large extent), Bureaucracy (78%-large extent) and identification of right stakeholders (77%-large extent). Procurement delays often refer to delay in receiving or obtaining certain things, software or hardware to complete the disaster recovery and business

continuity planning. The main general reasons observed behind a procurement delay are as follows (Lynch, 2015):

1. Delay in Preparing Technical Specifications, Scope of Work or Terms of Reference.
2. Failure to Start the Procurement Process on Time.
3. Extension of Bid or Proposal Submission Date.
4. Delay in Opening Bids or Proposals Received.
5. Delay in Starting or Finishing the Evaluation Process.
6. Delays during the Approval Process.
7. Delay in Contract Negotiations.
8. A Contractor, Supplier or Service Provider Challenges the Procurement Process.

Bureaucracy refers to a type of a team of government workers together involving in decisions without any consent from the elected people representatives. This means that there is a need for some consistency inside the government ministry to handle issues related to disaster recovery and business continuity. Many delays can be observed if there are disturbances in the bureaucracy form of decision-making happenings. The key to a successful governmental response depends upon the extent to which post-disaster human behavior corresponds to prior governmental expectations and planning (Schneider, 1992). There are pros and cons in terms of Bureaucracy as stated below (CliffsNotes, 2016):

Pros

1. This form of organization is not bad. For example, bureaucratic regulations and rules help ensure that the Food and Drug Administration (FDA) takes appropriate precautions to safeguard the health of Americans when it is in the process of approving a new medication.

2. Bureaucracy also discourages favoritism, meaning that in a well-run organization, friendships and political clout should not affect access to funding.
3. According to this research, bureaucrats have higher levels of education, intellectual activity, personal responsibility, self-direction, and open-mindedness, when compared to non-bureaucrats.
4. Another benefit of bureaucracies for employees is job security, such as a steady salary, and other perks, like insurance, medical and disability coverage, and a retirement pension.

Cons

1. Bureaucratic regulations and rules are not very helpful when unexpected situations arise.
2. One of the bureaucracy's least-appreciated features is its proneness to creating “paper trails” and piles of rules.
3. Critics of bureaucracy argue that mountains of paper and rules only slow an organization's capacity to achieve stated goals.
4. Approaching bureaucracies from yet another angle, the “Peter Principle,” named after sociologist Laurence Peter, states that employees in a bureaucracy are promoted to the level of their incompetence. In other words, competent managers continually receive promotions until they attain a position in which they are incompetent.
5. They also note that governmental red tape costs taxpayers both time and money.

Stakeholders are referred to none other than financial supporters or sponsors. They play a very important role in a business’s financial funding or support and towards the functioning of the business. Every project around the world would always consist of key stakeholders. They are

the main reason for the creation and conclusion of a project that people work on. They are in line with the top ladder people like CEO, CTO, etc... of the organization or company.

A few important notes can be recorded on how the stakeholders play a major role in a project. Look at the 4 Ways Stakeholders are Important to a Project (Schoenhard, 2005):

1. *Providing Expertise*: Stakeholders are a wealth of knowledge about current processes, historical information, and industry insight. Many times, these team members will have been at the company or on the project longer than the project manager or project team. It's important to involve all key stakeholders when gathering and documenting requirements to avoid missing major deliverables of the project.
2. *Reducing and Uncovering Risk*: The more you engage and involve stakeholders, the more you will reduce and uncover risks on your project. When discussing initial requirements, project needs, and constraints, stakeholders may bring up issues or concerns about meeting those things. Uncovering risks and then discussing a plan to mitigate them before issues arise will dramatically increase the success of your project. Involving knowledgeable stakeholders during this process will help.
3. *Increasing Project Success*: By gathering and reviewing project requirements with stakeholders, you will get their "buy-in," which will in turn help project success. If you can't meet stakeholders' needs, due to conflicting needs or priorities, set expectations early in the project life cycle. This will help you manage the relationship throughout the project instead of there being surprises at the end. Stakeholders should always be aware of the project scope, key milestones, and when they will be expected to review any deliverables before final acceptance.

4. *Granting Project Acceptance*: The more regularly you engage and involve stakeholders from the start, the more likely you will have a positive project conclusion. By the end of the project, the team members should have already been aware of delivery expectations, risks, and how to mitigate the risks. They also should have reviewed draft deliverables along the way. This process should help avoid any surprises at the end of your project. The final acceptance is just their final stamp of approval during the project closure phase.

This implies the importance of stakeholders needed in any situation involved in projects and can also be used as a resource in the disaster recovery and business continuity planning. The right stakeholders have to be identified and should be approached for. There are least effects in terms of change of project sponsor or change of government which gives a good sign that there are no issues with the project sponsor or the ruling government in there. But Procurement Delays and Beauracracy are the areas which have to be focused upon to get the Disaster Recovery and Business Continuity Plan working without any disturbances or lack of resources. The world is growing day by day, technology keeps advancing, and with this, there is rapid growth in the business industry around the world. More business is nothing but refers to more data and more resources. More data and resources refer to the need for security. To ensure security, disaster recovery and business continuity planning can help solving such issues which protect the data.

Chapter 4: Analysis of the Survey Results

Introduction

Various procedures or processes are followed by professional private and government organizations. These processes may fail unknowingly due to some external factors and thus brings down the business which is not good at all. When the business goes down, everything goes down financially, socially and publicly. With many disaster-related activities happening around the world, like cyber attacks, hacking, natural calamities like Earthquakes, Hurricanes, Storms there can be large effects to organizations. Hence to ensure safety, one must always build an efficient disaster recovery and business continuity plan and implement it with high importance. Business Continuity is mostly focused on operating in contingency mode where disaster recovery would refer to ensuring the protection of data, resources, and assets in terms of Information Technology.

Research Question 1

What are the business continuity and disaster mechanisms developed by Class A parastatals?

The answer to the above question can be understood from the Survey Analysis in the above section where it is seen that there are not many levels or layers of Disaster Management teams spread over in Kenya to sort out and develop proper Disaster Recovery and Business Continuity Plans. One can also infer that there are traditional ways that are mostly followed by the people in Kenya. Not much technology is observed in Kenya which means that there is not much advancement technologically. Nowadays, technology is reaching every corner and is making lives easy and comfortable. It reduces the workforce and automates thing. Kenya is a place where they are advancing in different fields like Telecommunications and Agriculture.

This would thus mean that Kenya would be easily able to adapt to new technology and stuff. For example, as per various articles over the website, one can see that in Kenya there are physical devices that are used to store data and then those physical devices are stored safely and ensured they are protected. Is it reliable? The answer is a simple NO in today's era where one can see cloud computing and other online storage services advancing around.

Nowadays, if you see things around, these cloud computing stuff and online storage services are seeming to be cheaper than using the physical devices to store data and protect them. Cost reductions are one of the major factors observed when using Cloud Services where this would help us get rid of physical locations or devices that are used to store and protect data. One can also know that there are many types of Cloud Services and it is mainly focused on our usage basis. You can select your required services only for your data. You will find different packages and stuff in Cloud Services around. So, the cloud services differ from organization to organization based on the size of data, number of resources or assets, etc.

While using Cloud services, one can also investigate the different approaches available where Cloud Services can be used as a primary recovery process and can also be used as a secondary recovery process which means "Backup." There are several external vendors and agencies who help in storing a backup of the data on the cloud, and the data would be used after the effects of disaster to recover the data. These vendors can be anywhere in the world, which is the best part.

There are many examples such as the 7.0 Magnitude Earthquake that shook off Alaska, Tsunami, Hurricane Michael, Hurricane Katrina, Hurricane Irma and Hurricane Harvey which happened recently causing effects on a big scale. Such kind of disasters can always fail an organization's disaster recovery and business continuity plan. Many things can be pointed out on

the weaknesses of the disaster recovery and business continuity plan built in. This means that it is always better to develop a proper disaster recovery and business continuity plan and ensure it is tested and maintained at regular intervals. Also, to include is to look out on technology advancements around which can help in time-consumptions and cost-reductions.

Cloud services are just an example where Kenya is not aware of. These cloud services are of such good help in Kenya and solve most of their data storage and protection issues. From the below picture one can see the different organizations involved in cloud services online helping organizations with managing their data and storing them with great protected features where no intrusions can happen, and these services are cost-friendly, trust-worthy and reliable.

	Managed Primary and DR instances	Cloud based backup and restore	Replication in the cloud
Instances	Email in the cloud	•On premises into the cloud •Cloud to cloud	•On premises into the cloud •Cloud to cloud
Merits	•Fully managed DR •100% usage based •Least complex	•Only requires cloud storage, cloud virtual machines are optional •Usually less complex than replication	•Best recovery time objectives (RTOs) and recovery point objectives (RPOs) •More likely to support application – consistent recovery
Caution	Service level agreements define access to production and DR instances	Less favorable RTOs and RPOs than replication	High degree of complexity
Implemented via...	N/A	Backup applications and appliances	•Replication software •Cloud gateways •Cloud storage software

Figure 9: Different available Cloud-based services as an example (Gsoedl, 2011)

Research Question 2

How can awareness and education be brought in at Educational Institutions and Government or Private Organizations operating in Kenya?

This phase where it discusses on Research Question 3 mainly focusses on technology advancements, why/what/when/how about Disaster Recovery and Business Continuity plans and previously failed situations while implementing the disaster recovery and business continuity plans. The previously failed implementations of a DR and BC plan would be one of the major contributions towards awareness and education in Kenya. That would include everything about the number of resources or assets used, the technology used, different types of services used in there, etc.

The top reasons organizations are failing to implement their disaster recovery, and business continuity plans are (Baxter, 2017):

1. Wrong decision making at the point of failure.
2. DR solutions are lacking adequate testing.
3. Changes in live systems not being updated on DR systems.
4. Data volumes and bandwidth restrictions.
5. False DR test reports.
6. Reluctance to invoke
7. DR solutions.

One thing that Kenya can focus on is to know what the basic steps are of understanding a disaster recovery and business continuity plan. What are the things to be kept in mind before commencing to understand the DR and BC planning? What comes to our mind first? Here one sees the six things that are to be considered while designing and prepping a disaster recovery and business continuity plan (Pace, 2015):

1. Identify and plan for your most critical assets.
2. Determine the Recovery Point Objective (RPO)/ Recovery Time Objective (RTO).

3. Scope out the technical mechanics.
4. Select an appropriate failover site.
5. Take advantage of the cloud.
6. The document, Test, and Refine.

From the survey analysis, one can observe that the testing phase and the implementation phase was not concentrated upon to a huge extent. And when coming to data storage techniques followed there, it is seen that according to the survey there was a very traditional formal backup policy and schedule followed and there were many backup tapes used which is a clear sign of how backward the situation is in Kenya in terms of technology advancement.

There are several ways to bring out awareness about disaster management which contributes towards educating the people in Kenya about Disaster Recovery and Business Continuity:

1. Public announcements through various sources media like the local TV Channels, local radio stations, newspapers and articles or magazines in stores and online.
2. Video advertisements being displayed on the TV channels and road-side displays is also encouraged.
3. Communicate with local market or store owners to set up some displays inside the store regarding disaster recovery and business continuity and educate the customers who come in.
4. Setting up some booths and help desks at schools, universities, and organizations can also be one of the good ways to educate working professionals and students.
5. Workshops where the actual process involved in disaster recovery and business continuity can be shown to people like the physical efforts and mental efforts needed

to be activated during a time of emergency. These workshops can be conducted at schools, universities and other private software organizations too.

6. Ensure a section about disaster management is added to the respective websites of schools, universities, companies and other residential areas where people who go through the website can have a look at it.
7. Communicate with the government disaster management teams and other related teams to gain more knowledge and ensure they are spread over to other people.

Research Question 3

What practices are used to create and implement business continuity and disaster recovery plans in Kenya? How would the plan be reliable and maintained, and how cost-effective the plan could be with dependencies over the resources and budget provided for the state organizations in Kenya?

From the above-discussed research questions, one can see how education and awareness can be spread over and how one can identify the different issues present in the locality. One can also see that the things in Kenya are mostly traditional or things are old-fashioned. So, one of the best ways here to start for Kenya is to adopt practices or procedures from other country's disaster management approach. Based on the other country's approach, the resources, assets and other things can be sorted out accordingly. As one sees through the Queensland Government's Disaster Management Plan, they are quite organized in terms of their planning procedures. The major points observed in their government's planning is discussed below to ensure Kenya can adopt a few things from them and be effective and efficient in their disaster recovery and business continuity planning.

Learning from other's success stories is always a positive thing which is what expected here. The procedures in the Queensland Government's Disaster Management is quite simple and comfortable to be followed. The below discussion would be helpful for organizations to make their disaster recovery and business continuity plan sustainable, reliable and efficient. They would also be gaining much knowledge regarding how to build and implement a disaster management plan by using the latest technology and other online cloud services.

"We cannot stop a natural disaster, but we can arm ourselves with knowledge: so many lives wouldn't have to be lost if there were enough disaster preparedness"–Petra Nemcova. The above suggests that knowledge is power. Using proper strategies in preparing a disaster recovery and business continuity plan always is helpful and useful to protect data, resources, and people —this way there should be some focus on disaster management planning in every organization. The government parastatals in Kenya have been practicing the disaster recovery and business continuity planning but in a traditional way which is a time-consuming process. They have a few resources which can be used to go along with the technology advancement and make processes look simpler. Traditional ways are outdated long ago. There are many features seen on the Queensland Government Disaster Management planning which can be inherited by the Kenyan Government Parastatals to ease processes up and create a better disaster recovery and business continuity planning. The features of the Queensland Government Disaster Management will be discussed below and would be seen to it as to how is it useful or helpful to the Kenya Government in their planning.

According to the Queensland Government, they mostly aim to fulfill three important things in their Disaster Management system (The Government, 2018):

1. The preparation of disaster management plans.
2. The matters to be included in a disaster management plan.
3. Other matters about the operation of a district group or a local group the Chief Executive considers appropriate having regard to disaster management for the state.

So firstly, the things considered here is the preparation of disaster management plans which means what factors must be considered and what type of guidelines need to be followed while creating a disaster management plan. Things that are needed to be discussed are how many people are to be required in this process and how many teams would have to divide the people into. The disaster management plan refers to a set of regulations or guidelines which are set to be followed during the time of emergency. Secondly considered here are matters to be included in the disaster management plan. So basically, we can see into the different points like:

1. The different kind of disasters to which the state faces the most in terms of human-made or unpleasant natural events.
2. What are the duties that would have to be performed at the state and central levels in such an unpredictable unpleasant event?
3. What is the present structure of the disaster management plan in terms of time-consumption, technology and resources?
4. What improvements or developments can be done based on the present status of disaster management planning.

The main officer leading this operation according to the Queensland Government is a Chief Executive for the Disaster Management Planning. One such experienced person can be chosen to lead the whole project of developing disaster recovery and business continuity planning. So, the Chief Executive would be the one responsible for figuring out the various

functions to be performed by specific teams at the state-level and central-level during the time of an unexpected unpleasant event. This means that the disaster management plan would be brought in at state-level and central-level with not much changes between them and which would bring in coordination and cooperation from the higher government officials too. A decision maker is always important in such projects in the form of a Chief Executive.

The disaster management planning of Queensland is mostly dependent on four principles as noted below (The Government, 2018):

1. Comprehensive Approach
2. All Hazards Approach
3. Local Disaster Management Capability
4. Support by the state group and district groups to local government

Comprehensive Approach

The comprehensive approach to disaster management comprises of four phases (The Government, 2018):

1. Prevention
2. Preparedness
3. Response
4. Recovery

The phases mentioned above were to ensure there is a balance of reducing the risk and focusses on ensuring real effective response and recovery responsibilities and capabilities.

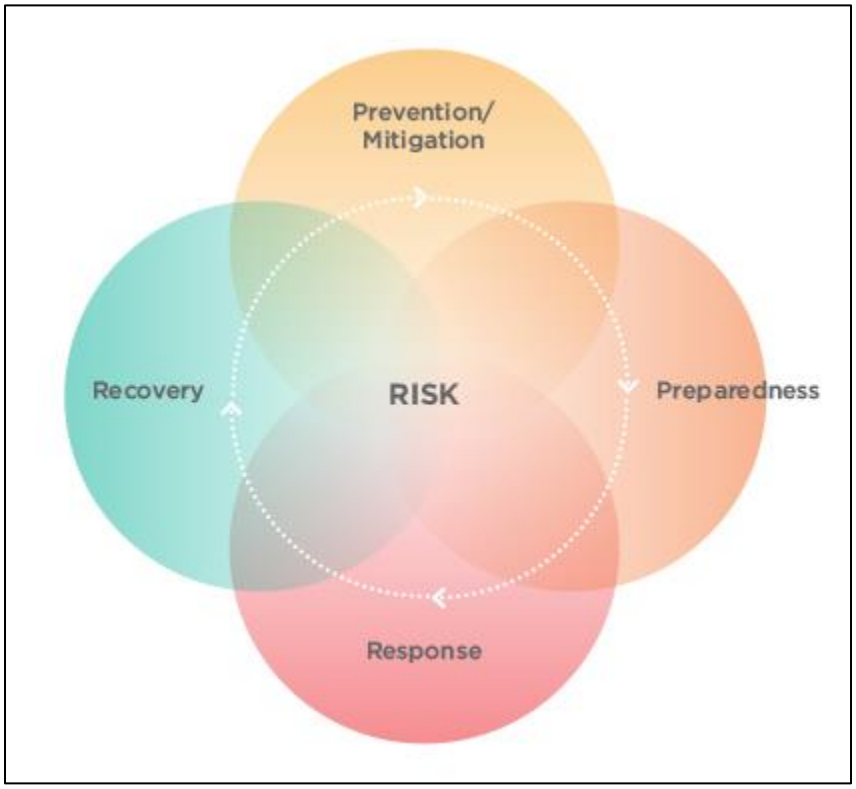

Figure 10: The comprehensive approach to disaster management (The Government, 2018)

Prevention/Mitigation: This refers to the different events which involve like preventing an unpleasant event from occurring, decreasing the percentage of chances of an unpleasant event to occur or decreasing the effect of damages that are done during an unstoppable emergency event. This phase mainly focusses on how to reduce the effects of an event which cannot be controlled completely. This phase helps us to be pre-planned to decrease the loss that is happening in the situation of an emergency or hazardous activity.

Preparedness: This phase is where one has to plan for the preparation of resources, testing, execution and proper cycling of the process in times of hazardous activities (human-made or natural). It considers various factors like organizing, training sessions, allocating of equipment and other resources, regular cycling of executing the plan and evaluation of the

various activities happening to face a situation. It mainly looks into the thing about how ready are we to face hazardous situations.

Response: This phase refers to an act of actions discussed in the Preparedness phase where all processes are executed in a timely and organized manner. It is the actual execution event where the disaster recovery and business continuity plans are executed to help reduce loss and ensure there is a business to be continued. It is a reaction to an unpleasant event like emergencies and hazardous incidents. It is about how well are you protecting lives, information, assets, and resources without much loss.

Recovery: This phase refers to the after effects of a disaster where things must be sorted out and should be brought back to normal functioning activities. Here it is focused mostly on how the processes can be brought back to its original phase where there is continuity ensured. This is where actually where everything is tried to be brought back to normal and ensure there is business continuity.

The comprehensive approach mainly focusses on what are the things that are to be done before an event occurs, during the event when it has occurred and what things are to be done after the event has occurred. This is the main phase where all the planning, organizing, resources, execution, testing, maintenance, financial-management phases are executed. Therefore, disaster recovery and business continuity planning should be considered in an organization to ensure the protection of lives and property to the maximum extent.

All Hazards Approach

This type of approach refers to disaster recovery and business continuity plan to be prepared in such a way that it can be executed in multiple kinds of disasters occurring. When a situation is considered, and a plan must be executed, one needs to make sure that the respective

plan in the event can also be applicable in another type of events which helps in time-consumption and financial-management which contributes towards smart planning of disaster recovery and business continuity planning.

Local Disaster Management Capability

This refers to the authorization of the local-level resources to be activated during the execution of the disaster management plan. This is mainly due to the knowledge available at local-level is quite high as they better know about their locality. This would mean that the local governments in their respective locations are responsible for their planning, preparedness and managing after-effects of a disaster irrespective of whether it is human-made or natural. This does not mean that the higher government levels are going to relax. The local government would be getting all their support they need from the higher government levels. This is mostly to recognize that the local government is the primary responsibility for disaster recovery and business continuity planning in their respective areas.

Support by District and State Groups

This refers to the thing as discussed above that the state and district-level disaster management groups are going to ensure all the arrangements are made to ensure that the local-level government ministries can effectively undertake disaster operations. An act or law should be created on how there should be effective coordination and cooperation between the state/district-level and local-level government ministries. In terms of extra support, central-level disaster management can also be involved to help during times of disastrous situations.

From the above approaches, one can understand how the planning of disaster recovery and business continuity plan can be done. Here one can see that there is a requirement of disaster management teams at the local level, state/district-level, and central-level and ensure there is

good coordination between all the various level government ministries. The main responsibility is handed over to the lowest-level government since they are their own best in terms of knowledge and can handle things in the best way and would need support from the high-level government support in terms of financial issues and resources required.

There should also be an eye out for continuous improvement in processes and on innovations happening in terms of technology. This refers to practice to take place where there is regular testing of the disaster management plan. It also would include various factors like looking out for improvements happening around in the world which could help us in developing our disaster management plans and ensure that they remain effective as usual as they were before. Innovation is where it is a search for creativity or other resources that they'll be able to grab up to include in their disaster management plan and make it more effective and fasten up processes to ensure positive outcomes from a disastrous activity event.

Learning and Education are also one of the important aspects required which contributes towards expanding knowledge and executing things in a better way where the disaster recovery and business continuity plan can be executed more effectively and ensure everyone is aware of what is happening around. Education is always important as they need to have enough knowledge about the different technologies, resources, and equipment that is being used in this disaster management plan execution during times of hazardous activities. This also contributes towards bringing in improvements and changes in the current disaster recovery and business continuity planning to see better outputs. This also encourages more people to be driven towards disaster management as a career in life and improve the percentage of employment and education. Education and Learning also provide good support towards better foundation on

disaster management planning where one can clearly understand the effects of hazards and contribute towards better disaster recovery and business continuity planning.

There are also disaster management structures which are discussed by the Queensland Government. The below important things must be set up in Kenya to ensure proper planning of their Disaster Management Plan. They are quite simple as discussed in the following points (The Government, 2018):

1. **Disaster Management Groups** that operate at local, district and state levels and are responsible for the planning, organization, coordination, and implementation of all measures to mitigate/prevent, prepare for, respond to and recover from disaster events.
2. **Coordination Centers** at local, district and state levels that support disaster management groups in coordinating information, resources, and services necessary for disaster operations.
3. **Disaster Management Plans**, developed to ensure appropriate disaster prevention, preparedness, response and recovery at local, district and state levels.
4. **Functional Lead Agencies** through which the disaster management functions and responsibilities of the state government are managed and coordinated.
5. **Hazard-specific primary agencies,** responsible for the management and coordination of combating specific hazards.
6. **Specific-purpose committees,** either permanent or temporary, established under the authority of disaster management groups for specific purposes relating to disaster management.

So, from the above discussions, one can see how different the structure between Queensland and Kenya. Firstly, the disaster management groups or teams available in Kenya is not organized, and not much coordination is seen between the state and central level governments. The knowledge available in these places is quite low which is why no improvement is seen in term of disaster management and business continuity planning. The other obvious thing one can observe is the use of technology which is where Kenya is quite behind, and they must ensure usage of all the latest software or technology available to better their planning procedures. External vendors can also be used in this process which is a very good way as they are the professionals in their work and have the knowledge to get data and information stored safe and secure. The Queensland Government has also discussed regarding the major factors of Prevention, Preparedness, Response and Recovery which we have already discussed in the above sections of this paper. Many important features can be adapted from the Queensland Government's Disaster Management planning and can be applied to ensure time-consumption measures and cost-reductions on the run.

Summary

This chapter identifies the different options available for Kenya from which they can adapt features to ensure proper planning and implementation of a Disaster Recovery and Business Continuity Plan. The coordination and functioning of different level governments have been discussed which is also one of the major factors in here. The different governments are the local-level, state-level, district-level governments. This chapter provides us with information regarding the three research questions that were quoted in the above sections. These three research questions are mainly dependent of how to identify issues or concerns in a locality in terms of resources or assets, how to educate or bring awareness among people regarding Disaster

Recovery and Business Continuity and what best practices and recommendations can be turned in to better the planning processes or procedures in Kenya. Since Kenya is a developing the country and has been seeing more and more business and information coming into the country, they must be prepared for worse case scenarios too. This chapter focusses on the need for Cloud Computing services to be used and how well they can adapt from the Disaster Management planning of the Queensland Government.

Chapter 5: Recommendations, Future Work, and Conclusion

Introduction

This chapter is focused on the overall thoughts and comments done based on the above-discussed chapters about Kenya Class-A parastatals which are referring to Kenya Government. The status of their disaster recovery and business continuity planning is discussed and how it can be improvised is what is studied here. There is always a scope for learning, and there is no end to it in the present era where one sees a lot and a lot of developments and advancements going on around in the world. Innovations and automation are always improvising and getting themselves to new heights with great innovation and creativity. This chapter thus focusses on the recommendations and conclusion of our research. Thus, disaster recovery and business continuity plans in Kenya are studied and investigated to provide solutions to how they can better their planning.

Recommendations

The basic recommendations to be discussed here is the need for cloud computing services and new technology which is one of the major factors in the process of planning of efficient disaster recovery and business continuity plan. Another major factor to be considered here is to perform the Business Impact Analysis which helps identifies the various factors about prioritizing business processes and identify the weaknesses and loopholes in the company or organization where data or information and resources would be compromised. This study also recommends Kenya to get away from traditional ways of storing data and protecting through physical devices like backup tapes and hard drives. There are cloud computing services which are now available all around the world which was discussed in the above sections. These cloud computing services can be adapted by the organizations in Kenya themselves or can also consult

local or international vendors for these services. These services can be provided from any part of the world which is one of the best features. All the data and information is going to be stored on the cloud without any interruptions in the current business processes and is safe and secure. This study also recommends for effective planning, proper testing, and regular updates/upgrades if any. Planning and Testing are one of the main phases which are important in implementing disaster recovery and business continuity planning. The disaster management planning of Queensland can always be a good reference for effective and efficient disaster management approaches.

Conclusion

Disaster Recovery and Business Continuity Planning has always been one of the major elements contributing to the success of an organization. In today's world, there is a huge competition between companies or organizations which makes this an important factor of developing an effective disaster management plan to ensure data protection and resource safety. In this paper, the notes discussed are about the weaknesses and strengths of the disaster management approach followed in Kenya mainly by their government ministries. Observations have inferred that the approach in Kenya is old-fashioned and recommendations and practices have been defined to ensure effectiveness and efficiency in their disaster recovery and business continuity approaches. Various factors about the Queensland Government's Disaster Management approach and cloud computing services has been discussed where Kenya can prioritize their concentration towards and implement these developments for better disaster recovery and business continuity planning. One can also find many organizations that are good enough in sharing their standards and procedures of preparing, developing and implementing disaster management approaches. Organizations must always keep an eye out on the

developments and advancements happening around in terms of technology and on the standards and procedures followed by other organizations especially from developed countries like United States of America, United Kingdom, etc. To be short, there is a need for proper and effective disaster recovery and business continuity plans to be deployed by organizations to ensure their business is in safe hands even after an occurrence of natural or human-made disasters.

Future Work

There is always scope on future work where other automation advancements are happening around to reduce time-consumption and cost. Online services are developing around to make things easier and comfortable where one of them are cloud computing services. There are more and more vendors growing up to ensure data storage and protection. Many software and coding languages are being built up to help automate things more effectively. One can also see growth in Artificial Intelligence where we see autoboots or robots being created to help automate certain processes in our day to day life. Future is always bright, and there are many developments to keep an eye out for. This study is about how the Kenya government ministries can improvise their planning towards disaster recovery and business continuity.

References

Baseline. (2015, November 26). *Why disaster recovery testing is a standard procedure.* Retrieved from Baseline Data Services, LLC: https://baseline-data.com/blog/disaster-recovery/testing-your-recovery-system-when-and-why/

Batson, A. (2017, March 21). *4 Major risk of not having a business continuity plan*. Retrieved from Preparis: https://www.preparis.com/blog/4-major-risks-not-business-continuity-plan/

Baxter, B. (2017, July 5). *6 reasons why IT recoveries fail.* Retrieved from CSO (from IDG): https://www.csoonline.com/article/3205248/backup-recovery/6-reasons-why-it-recoveries-fail.html

CliffsNotes. (2016). *Pros and cons of bureaucracy.* Houghton Mifflin Harcourt.

CyberSponse. (2017). *The lifecycle of "incident response" and building an effective plan.* Retrieved from Cybrary: https://www.cybrary.it/channelcontent/lifecycle-of-incident-response-and-building-an-effective-plan/

EzeCastle. (2018). *Eze business continuity planning.* Retrieved from EzeCastle Integration: https://www.eci.com/products-services/business-availability/business-continuity.html

Fujitsu. (n.d.). *10 top tips for data protection in the new workplace*. Retrieved from Fujitsu Technology Solutions Gmbh: http://www.fujitsu.com/us/Images/33440_T4B_ Security_brochure_-_pdf.pdf

Gahler, M. (2016). Remote sensing for natural or man-made disasters and environmental changes. *INTECH (Open Science | Open Minds)*.

Gregg, M. (2009). Business continuity and disaster recovery planning. *Pearson IT Certified Article*.

Gsoedl, J. (2011). *Disaster recovery in the Cloud explained.* Retrieved from Tech Target: https://searchdisasterrecovery.techtarget.com/feature/Disaster-recovery-in-the-cloud-explained

Huho, J. &. (2016). Profiling disasters in Kenya and their causes. *Academic Research Internationa,. 7*.

Investopedia. (2018). *Business Continuity Planning (BCP).* Retrieved from Investopedia: https://www.investopedia.com/terms/b/business-continuity-planning.asp

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

Lynch, J. (2015). *8 causes of delays in the public procurement process and how to avoid them.* Retrieved from The Procurement ClassRoom: https://procurementclassroom.com/causes-of-delays-in-public-procurement/

Martin, B. C. (2002). *Disaster recovery plan strategies and processes.* SANS Institute InfoSec Reading Room.

Mathenge, M. W. (2011, October). *Disaster recovery and business continuity plans in class-A parastatals in Kenya*. (Thesis), University of Nairobi.

Milledge, J. (2015). *Disaster management concepts*. Retrieved from SlidePlayer: http://slideplayer.com/slide/1520375/

Nalo, D. S. (2007). The place of ICT in growth of business - Kenya's vision 2030 in perspective. *Annual Strathmore ICT Conference*.

Pace, A. (2015, November 23). *6 things to consider while designing and prepping your disaster recovery plan.* Retrieved from SINGLEHOP (an INAP company): https://www.singlehop.com/blog/designing-your-disaster-recovery/

Professionals, I. (2016). *IT network disaster recovery.* Retrieved from Advanced Computer & Data Communications: http://acdcommunications.com/disaster-recovery.html

Riolli, L. (2003). *Information system organizational resilience* (pp. 227-233). California: Omega. 31.

Rutledge, L. (2014). *Disaster recovery & business continuity - did you validate?* Retrieved from LearnAboutGMP: https://learnaboutgmp.com/software-validation/disaster-recovery-business-continuity-did-you-validate/

Schneider, S. K. (1992). Governmental response to disasters: The conflict between bureaucratic procedures and emergent norms. *JSTOR*, 11.

Schoenhard, L. (2005). *4 ways stakeholders are important to a project.* Retrieved from Proficient Learning: https://proficientlearning.com/4-ways-stakeholders-are-important-to-a-project/

Taylor, P. B. (2013). Business impact analysis for the city of Virginia Beach. *The City of Virginia, Communications and IT*, 209.

The government, Q. (2018, September). *Queensland government disaster management.* Retrieved from https://www.disaster.qld.gov.au/dmg/Introduction/Pages/1-2.aspx

Tittel, K. L. (2017, July 18). *How to create an effective business continuity plan.* Retrieved from CIO (From IDG): https://www.cio.com/article/2381021/best-practices/best-practices-how-to-create-an-effective-business-continuity-plan.html

Valent, N. (2016, July 14). *The top three challenges to developing a business continuity and disaster recovery plan.* Retrieved from OnRamp: https://www.onr.com/blog/top-three-challenges-developing-business-continuity-disaster-recovery-plan/

Venclova, K., & Vydrova, H. U. (2013). *Advantages and disadvantages of business continuity management*. World Academy of Science, Engineering and Technology.

Virginia Cerullo, A. (2004). Buiness continuity planning: A comprehensive approach. *Semantics Scholar*, pp. 70-78.

Voorde, M. M. (2014). *Maintenance and engineering: Key players in emergency preparedness.* Retrieved from faciltiesnet: https://www.facilitiesnet.com/emergencypreparedness/article/Maintenance-and-Engineering-Key-Players-in-Emergency-Preparedness-Facility-Management-Emergency-Preparedness-Feature--14824

Wunnava, S. (2011). *Application of protection motivation theory to study the factors that influence disaster recovery planning: An empirical investigation.* ERIC.