A SURVEY OF INFORMATION AND COMMUNICATION TECHNOLOGY ASPECTS OF DISASTER RECOVERY AMONG COMPANIES QUOTED AT THE NAIROBI STOCK EXCHANGE

BY

AGNES NYAMBURA

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION (MBA),
FACULTY OF COMMERCE,
UNIVERSITY OF NAIROBI

NOVEMBER 2005

DECLARATION

This project is my original work and has not been submitted for a degree in any other University.

Signature ..... **Date** ...15...Nov...2005.....

Agnes Nyambura

This project has been submitted for examination with my approval as University Supervisor.

Signed ..... **Date** 15th November 2005

Mr Joel K Lelei

Department of Management Science

Faculty of Commerce, University of Nairobi

DEDICATION

This work is dedicated to the Lord for His mercy and favour upon my life and for the graces He has continuously bestowed on me. Secondly, I dedicate this work to my beloved husband Andrew and our two children, Maryann and Morris for the love, patience, understanding and support they have shown me during the entire period of study and until the finalisation of this research project.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

My sincere and heartfelt gratitude is extended to Mr Joel Lelei for supervising this research and for the support he has given throughout the entire period, I appreciate the invaluable advise, comments suggestion, corrections and directions he has extended to me. I also appreciate my husband, Andrew for his effort in ensuring that I had all the facilities to ease my finalisation of this research. I also acknowledge the efforts of Mr T. Akama, for accepting to proof read and extend suggestions for corrections.

ABSTRACT

The objectives of this study were three. The first was to establish the aspects of disaster recovery that exist within companies quoted on the Nairobi Stock Exchange. The second was to determine the importance attached to the aspects of disaster recovery. The third was to determine the challenges faced by IT managers in companies quoted on the Nairobi Stock Exchange in implementing disaster recovery aspects. The need for this study arose due to the fact that, different organisations have unique business needs in view of the Kenyan social economic and legal context.

Companies are increasing being faced with the threat of disasters that could interfere with the normal operations of the business. This has thus, created in increased need for organisations to put in measures to be prepared for business continuity in event of a disaster. Each organisation has different aspects of disaster recovery and each may rate different these aspects differently in view of the unique challenges that they face. To determine the aspects in these organisations and the relative importance they assign to them as well as the challenges they encounter, a structured questionnaire was administered to Information Systems Managers in all listed companies whose shares were actively traded at the Nairobi Stock Exchange.

The results show that, the aspects that are most critical are management support, risk analysis and business impact analysis and thirdly, having a disaster recovery plan. Management has the responsibility to ensure that, the organisation is continually being able to carry out it business relationship through availability of data and information to make business decisions. Therefore, it is integral that, management is involved in disaster recovery as they have the responsibility to develop, approve and enforce the disaster recovery programmes and create support for the same amongst the employees.

The results also indicated that, the risk and business impact analysis would enable the business identify the threats it is faced with and also evaluate its critical business data to

ensure that the same is protected by having measures in place that would ensure availability of data for purposes of business continuity.

The data also showed that, creating a disaster recovery plan is critical for all businesses as it enables having procedures to follow in event of a disaster as well as putting in place mitigation measurers to reduce the impact of a disaster on the business. Creating a disaster recovery plan would highlight the need to have a disaster recovery team in place that would have the responsibility of guiding the business in event of a disaster with the relevant team members having specific responsibilities in view of their skills and expertise. The plan would highlight the need for training of all employees to be sure that there are aware of the plan and they understand what would be expected of them in event of a disaster event. It would also ensure, that testing is done to enable updating of the plan such that it can be used in event of a disaster because it would be relevant and current.

The challenges that most organisations undergo as highlighted from the results are lack of management support, lack of carrying out impact analysis, and lack of implementation and ongoing management.

The survey study was carried out amongst companies quoted on the Nairobi Stock Exchange and it was realised from the results that overall, quoted organisations are aware of the need to have disaster management programmes within their organisations for purposes of preparation.

LIST OF TABLES

LIST OF ABBREVIATIONS USED

BIA	Business Impact Analysis
CEO	Chief Executive Officer
DR	Disaster Recovery
DRP	Disaster Recovery Planning
IS	Information Systems
IT	Information Technology
NSE	Nairobi Stock Exchange

CHAPTER 1: INTRODUCTION

1.1 BACKGROUND

Information is regarded today as a fundamental factor of production (Hannabus, 1987). Its role as an important organization resource just like land, capital and labour is increasingly being realized and as Drucker (1987) puts it, "the computer is just an aid, it is the information that counts". However, the technology on which it is based is facing crises. Indeed, technology-based crises are on a rise, and will continue to rise as technology immerses and becomes a fabric of our societies. Thus, organisations need to prepare for crises. As Desouza (2004) notes, the recent surge in viruses, network failures, data losses and leaks, sabotages to networks, and many other malicious acts are witness to the increasing need for organizations to prepare for technology-based disasters.

A disaster can be defined as the occurrence of any event (accident, catastrophe, tragedy, or emergency) that causes a significant disruption in information and communication technology capabilities. It is typically an event that disrupts the normal course of business, making the continuation of normal functions impossible to the extent that monetary losses can be quantified (Bates, 1991).

The use of the words "disaster" and "recovery" imply that, everyone is destined to live through a disaster in his or her lifetime. Myers (2003) explains that disaster recovery (DR) is "the ongoing process of planning, developing, testing, implementing key business technologies to ensure the resumption of vital business functions in the event of a declared disaster".

For purposes of this study, disaster recovery shall be defined as mitigation of a disaster or response to a declared disaster to ensure business continuity. It is the organisation's ability to continue its day-to-day operations, despite an occurrence of a catastrophic nature through a series of co-ordinated and pre-planned activities with the awareness and endorsement of senior management.

According to Heidelberg (2003) now, more than ever, Information Technology (IT) managers need to make certain that their organisations continue to function after minor incidents or major disasters - from slight data loss to natural events or terrorism. This can be achieved by developing a proper disaster recovery management program.

There are aspects that are crucial to the success of a disaster recovery management programme. The successful planning and implementation of a DR management program requires support from the management. Therefore, the information and communication technology section which plays the main role in overall planning and leading disaster recovery planning (DRP) initiatives should ensure that management is involved. This is because they are better placed to give authority to do what is necessary and gauge the business impact. They should also be trained and briefed on the progress of the program adequately to ensure support.

According to Maiwald and Sieglein, (2002) a disaster recovery team is the core of the organisation's response to a disaster. The team provides the leadership and authority to do what is necessary to correct the problem and accomplish the goals of the organisation during the incident. It is, therefore, important that the team be made up of appropriate individuals, with strong leadership and who have the proper authority to carry out the team's work. It should consist of representation from all areas of business within the organisation and it is important and critical that it is prepared for an incident. Testing the DR team and drilling the procedures is absolutely essential to make the team function properly.

During the business impact analysis (BIA) and risk assessment, the DR team needs to help in answering critical questions about the potential consequences of system downtime. The BIA would help develop a clear understanding of the business by identification of the critical assets and data as well as essential items for the survival of the business. This is critical for developing an effective disaster recovery plan.

Contingency plans provide the organisation with necessary information to not only respond to emergency or disaster, but also to recover and resume operations of the critical services that the organisations provide. Therefore, developing policies and procedures is critical to laying out step-by-step methods designated to restore an organisation's functions or business processes in order to recover from a disaster (Koehler, 2002).

Testing the plan and drilling the procedures is absolutely essential to making all the people involved function properly. Testing enables identification of improvement areas as well as updating the plan. All employees should be aware through training of what is expected of them in terms of preparing for a disaster and how to respond if one occurred (Desouza, 2004).

The importance of the aspects of disaster recovery are all geared towards preparing for, responding to and recovering from a variety of disasters. The management provides guidance and support to the DR team, which ensures that the BIA has been carried out in order to identify critical and essential business processes and functions. The policies and procedures ensure that roles and responsibilities have been doled out in order for recovery procedures to be carried out correctly. Ongoing cycles of training, drills, exercises and tests followed by corrections and enhancements ensure that the organisations plans and procedures and response capabilities continue to improve (Kildow, 2002). The above would then translate to advantages including: competitive advantage, protecting the company image, avoiding loss in revenue and customers' loyalty, avoiding legal implications, meeting the regulatory requirements and overall, for company survival.

However, there are challenges to disaster recovery management which include: limiting the scope of DR to the IT department instead of dealing with it at an organisation wide level; lack of proper funding for DR management, lack of commitment from management, lack of technological and human resources expertise and lack of employee involvement who should be educated on the importance of compliance to disaster recovery procedures.

This research is to be carried out among companies whose information technology systems are ICT based in different industries in order to evaluate whether they are prepared to mitigate disaster and/or deal with a disaster if it does occur. Therefore, companies listed on the Nairobi Stock Exchange (NSE) are appropriate for this study. The NSE was registered in 1954 under the Societies Act and later in 1991 under the Companies Act with the objective of dealing in shares, stocks and other capital forms through a formal market, with rules and regulations to govern stock broking activities of its members. The publicly quoted companies (48) are divided into five sectors namely: agricultural, finance and investment, commercial and services, industrial and allied and Alternative Investments Market Segment.

Quotation status accords firms two significant benefits: first, quotation at the stock markets promotes higher standards of accounting and resource management. This is because stock markets encourage the separation of ownership of capital from management of capital. This separation is important as the stock exchange as it forms a link to entrepreneurs with bright business ideas but without capital to invest, thus, upscale management of such organisations.

Secondly, publicly held firms being under the scrutiny of watchful investors are likely to be among the well run businesses in the private sector and are therefore likely to take the lead in adopting and implementing aspects of disaster recovery for the continuity of their businesses.

Given their size and quotation status, these firms may be expected to have the basic infrastructure to support disaster recovery programmes.

1.2 STATEMENT OF THE PROBLEM

Disasters of all shapes and sizes occur to businesses and can lead to "death of the business". Therefore, as organisations have become so dependent on the IT infrastructures, it is essential that they develop and keep an up to date IT disaster

recovery management program. This is inevitable for the continuity of any business given that IT is very vulnerable to disasters.

IT based disaster recovery management consists of a number of aspects which vary with respect to respective organisation's business functions and needs. Managers are faced with the question of what the important aspects are in regards to their different business functions and needs.

IT managers should identify the importance of aspects of DR in respect to their assets and data in order to put together a contingency plan to deal with recovery and restoration (Sieglein and Maiwald, 2002)

It is important to note that, the solutions in the market today that cannot lay out every single aspect of DR planning solution for every business and scenario because every organisation is unique in terms of its business processes and needs. Therefore, every organisation needs to customize its own plan: one that makes allowances for its own set of corporate factors that are inherent to its success. This raises the question of challenges that managers face in tailoring those issues that have greatest impact to an individual business when preparing the disaster recovery programme (Miano, 2003).

In Kenya, a number of companies and institutions have adopted IT each to differing extent. The use of computers, telecommunications or a combination of both in any given company differs on the level of sophistication. However, the extent to which technology has been adopted is not documented. In view of the adoption of information technology, some companies have disaster recovery programs but others do not have such programs put in place (Mutunga, 2004). The focus on disasters of whichever nature is therefore necessitated by the need for sensitisation on the precautionary options available for individuals and organisations, especially in urban set-ups. This is as there are no efficient detection systems and/or well co-ordinated actions that can help tell whether there is a change in disasters, and if so, by how much.

According to Mawanda (2004), there is no Disaster Management Act and it is the reasons why individuals and organisations that have the disaster recovery management programmes either finance themselves through grants or loans without a steady budgetary allocation that would have been possible if there was a Disaster Management Law.

Studies focused on disaster recovery or management of disasters in general may not be expected to fully explain the aspects of disaster recovery in terms of information technology in companies quoted on the Nairobi Stock Exchange. Thus, the aspects of disaster recovery require a separate study in view of the unique business needs. This means that, research results from other contexts may not reflect the aspects of disaster recovery of information technology in a probably unique Kenyan social economic and legal context though they have provided a base for the current study.

Therefore, a research is called for, where none has been done in Kenya to the best of my knowledge. The fundamental questions addressed by the study are: what aspects of disaster recovery are crucial; what is the importance attached to these aspects and what are the challenges that managers face in effecting disaster recovery programmes.

1.3 OBJECTIVES OF THE STUDY

The objectives of this study include:-

a) To establish the aspects of disaster recovery management used by companies quoted on the Nairobi Stock Exchange;

b) Determine the importance of aspects of disaster recovery management as considered by companies quoted on the Nairobi Stock Exchange; and

c) Determine challenges faced by IT managers in companies quoted on the Nairobi Stock Exchange in effecting disaster recovery programs.

1.4 IMPORTANCE OF THE STUDY

The study is of value to various interest groups including:

a) Managers of various companies that intend to adopt or have already adopted disaster recovery practices in their companies would be interested in the findings

of this study. They could draw upon the findings in setting up strategies for enhancing their disaster recovery management programs;

b) To the Government of Kenya, the Kenya Computer Society and other bodies involved in ensuring disaster recovery management, the findings of the study will help come up with a national policy framework and strategy for IT disaster recovery;

c) To the academia, the study will add to the existing body of knowledge as well as serve as a foundation to carrying out further research in this wide area.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

Disaster recovery and business continuity planning are basic realities that businesses, large and small, need to address in order to maintain operations before, during, and after a catastrophic event. However, these have to be tailored to address those issues that have the greatest impact on an individual business (Miano, 2003).

Business continuity is the overall process consisting of disaster recovery, business recovery, business resumption, and contingency planning (Maiwald and Sieglein, 2002). Therefore, "organisations of all sizes should have a business continuity plan; not having one is cavalier at best, negligent at worst" (Sharp, 2003).

The ability of business managers to gauge the value of their data correlates to the success of the company's business continuity and data recovery efforts though it is hard to provide such a gauge given the massive amounts of data coursing through organisations and the fact that the value of data changes frequently and quickly in today's unpredictable, highly competitive, and increasingly regulated business environment (Croy, 2004).

IT managers typically plan for systems recovery in the event of some kind of network outage. But they often do not take the next critical step – ensuring business continuity and operational functions. In stopping short, they put the company at risk of losing customers, reputation and revenue (Southgate, 2002).

Therefore, the need for disaster recovery planning is realised. DR planning should be aimed at the definition of business processes, their infrastructure supports and tolerances to interruptions, and the formulation of strategies for reducing the likelihood of interruption or its consequences (Maiwald and Sieglein, 2002).

Organisations that operate without a DR program are likely to go out of business within a few years when disasters strike. A research group, Gartner, estimates that two out of five companies that experience a disaster go out of business within five years. Worse still, it is estimated that 60 percent of businesses either operate without a disaster recovery plan and those with a plan, have never tested it or it failed upon testing.

In spite of the grim statistics, many companies are gambling with their survival by failing to carry out the necessary steps to protect their operations against disaster to ensure seamless recovery when it does strike.

By now, information technology executives all over the world know that having a plan in place for recovery from unexpected outages, either natural or man-made is vital to the health of their business. The volume of information continues to increase as a result of e-commerce and other business critical enterprise applications, along with businesses and consumers demanding protection of this data and access at all times. Consequently, information technology departments must implement disaster recovery networks while simultaneously managing the cost of expanding storage and network infrastructures with tight or shrinking budgets (Bird, 2003).

The review shall present the literature pertinent to the subject of the study. The aspects of disaster recovery and their importance shall be discussed and thereafter, the challenges that are experienced in effecting a disaster recovery programme shall be discussed.

2.2 ASPECTS OF DISASTER RECOVERY

2.2.1 Management Support

Management plays several roles in policy implementation. Management must approve and enforce policy and must help develop and approve the written disaster recovery policy. Once the policy has been approved, they are the ones that must help ensure that the policy is understood by their staff, participate in following the procedures for each policy, and enforce the policies when necessary (Maiwald and Sieglein, 2002).

A solid DR program requires the support and participation of business managers and executives. The implications include the fact that implementing the plan and responding to disaster is an organisation wide effort, plan development requires many types of knowledge and skills and the fact that every organisation-wide effort is laden with social and political obstacles that need to be addressed during planning. Therefore, managers should be well informed about the criticality of the information technology systems they rely on to provide data for decision making and the impact any downtime would have on the business.

To support the plan adequately, the executives need training to articulate the organisation's philosophy for disaster recovery planning. They should also be briefed on the progress of the plan.

There should be appropriate statements on the organisation's disaster recovery planning for executives to deliver to the board of directors, investors the media and general public. Thus, appropriate contacts in the organisation should be determined to answer detailed questions regarding DRP and ensure that outside parties are properly referred for answers to these questions (Maiwald and Sieglein, 2002).

Chandler and Wallace (2004) reported that organisational commitment to disaster recovery planning after the events of September 11 had increased companies' commitment, sense of urgency, and intensity of disaster recovery planning. The attacks appeared to have increased the profile of disaster recovery planners in most organisations and made the disaster recovery plans an urgent item for strategic planners across industry sectors.

2.2.2 Disaster Recovery Team

The DRP team should be a well-rounded group that represents all the functions of an organisation thus ensuring that essential business processes are not overlooked during plan development (Maiwald and Sieglein, 2002).

The team also requires a high level manager as a champion, ideally the Chief Executive Officer (CEO) or a high level manager designated by the CEO to publicly support and endorse the plan as well as eliminate issues that hinder its development.

The team has the responsibility of ensuring that they get support from the executives in terms of resources, participation and co-operation needed to create a successful plan. The team should be trained in order to understand the issues and basic concepts of DRP (Maiwald and Sieglein, 2002).

They could develop appropriate statements on the organisation's disaster recovery planning for executives to deliver to the board of directors, investors the media and general public.

At the same time, the team should establish an awareness campaign about disaster recovery planning within the organisation so that all employees are aware of the programme and well as gather their support.

2.2.3 Business Impact and Risk analysis

Bates (1991) says that, the identification of critical assets and data is crucial to creating a functional and effective disaster recovery plan. Part of determining items that are critical and essential to a business is in doing a business impact analysis. It is essentially a means of systematically assessing the potential impacts resulting from various unavailability events or incidents.

Risk analysis helps establish a good security posture while risk management keeps it that way (Jenkins, 1998). In general, risks can be categorised into three: risks that affect business operations, risks that affect the physical facilities and environments and risks that affect personnel, health and general public. Therefore, risk analysis enables identification of the magnitude of risk that could arise due to the different impacts thus enabling identification of scenarios that are most likely to occur in practice and which should therefore require more attention during planning.

Prudent risk management takes into consideration those measures that when implemented, can best manage and reduce the risk factors with which the organisation is already familiar. These factors may include: backup strategies that reflect the critical nature of data, comprehensive knowledge of interdependencies with other organisations that may be affected, thoughtful considerations of geographical environment and risks, and the knowledge of available supporting infrastructure for example, telecommunication networks etc.

A BIA thus clarifies the degree of potential loss and unwanted effects, which could occur. This covers reputation damage, regulatory effects, financial impact to the organisation resulting from business unit's inability to conduct their operation, operational impact relating to each business operation, current state of preparedness to resume business operations, technology requirements for resumption and recovery and information systems support for resumption of time sensitive operations.

The BIA is important in that, the data collected is pivotal to collecting the key business issues and justifying the resources needed to mitigate business risks. It provides the following: identity of time sensitive business operations and services, analysis of the organisations financial exposure and operational impact, the time in which time sensitive operations, services and functions must resume, and an estimate of the resources necessary for recovery, resumption and restoration (Bates, 1991).

Most organisations have long been aware of the business impact of an unplanned outage to computers and communication based systems. There is a realisation that an event like the September 11 attack requires that organisations not only focus on their own individual recovery plans but, must also consider how the recovery efforts of other companies in their industry, customers, suppliers or supporting industries must be coordinated so that normal or near normal operations could resume. They must also realize the impact on public infrastructures could have an impact on their individual or collective abilities to recover (Jackson and Dec, 2002).

The BIA thus provides the rationale and justifications for risk mitigation and response, recovery and resumption decisions.

2.2.4 Contingency Plans and Procedures

According to Bates (1991) a disaster recovery plan describes how an organisation is to deal with potential disasters. Myers, (2003) says that, a disaster recover plan is "a living document designed to guide the team through a declared disaster". Therefore, the lack of a plan leads to extended periods of downtime causing chaos in the environment, loss of customer, shareholder and employee confidence in the organisation.

Myers (2003) and Miano (2003) both agree that, there are some major considerations that should be addressed when developing a disaster recovery plan which include: -

Firstly, the safety of company employees and their ability to perform the necessary recovery work is crucial. Organisations should consider potential problems to their employees and incorporate suitable allowances when developing staffing requirements into recovery plans. The organisations should also realise that communication is key – an organisation should be able to contact its employees after a disaster, therefore, when developing a recovery plan, the phone lines and other critical communications should be taken into account. Up to date records of employee cell phone numbers and 'back-up' numbers should be kept. It is also important that the company's management be pro-active in communicating the firm's ongoing status and situation to employees. In view of the above, it is a good idea to designate several individuals as the company's authorised representatives for dealing with the media. They should be adequately prepared to present the firm's efforts and situation in the best light possible.

Secondly, companies should back up all critical, corporate data and information in alignment with business deliverables and also ensure that the company's technology is protected.

Thirdly, successfully returning key company data and information to its original state is critical. If infrastructure recovery is out of a company's hands, plans should be made accordingly for example, communication issues, power requirements. It is thus important to recover the work within the amount of downtime allowed (as defined by business needs).

Fourthly, performing scheduled plan testing to helps validate the above three issues. All employees should read the document for accuracy and practicality. Walk-throughs and regularly schedule annual tests should be carried out to determine the plan's effectiveness and implement modifications that would be needed.

Finally, it is important to define and practice ongoing disaster recovery planning training for new and existing employees. It is imperative that, more than one company employee is capable to implement company critical functions. Every employee who is expected to actively participate in the company's recovery after a disaster must have their own copy of the plan. They should be fully aware of their roles and responsibilities should a disaster occur (Myers and Miano, 2003)

The contingency plans should derive from existing policies and procedures with roles and responsibilities for preparing for, responding to and recovering from a variety of disasters. Policies are the guidelines that govern the development of disaster recovery procedures. The procedures are step-by-step methods designated to restore an organisational function or business process. It is, therefore, important to critically evaluate all facilities and business operations to determine what kind of procedures must be developed to facilitate recovery.

A comprehensive plan that accounts for all eventualities is a corporate need. Thus, the procedures and plans should be clear and concise so that employees can quickly refer to them and understand their responsibilities during response and recovery. The procedures should also clearly highlight communication with employees, the media, law enforcement

and emergency services. It is critical to have proper documentation of all procedures and this should be managed in terms of reviews, updates and approvals.

The roles to be played by interdependent organisations should be defined in order to evaluate risk of threats from them. These include suppliers, outsourcers, brokers and others that are required for an organisation to be efficient in today's world.

In comparing the preparedness for disaster in 2001 and 2004, Chandler and Wallace found that, more companies have a written disaster recovery plan in 2004. They also found that by many measures, preparedness had improved in the years since the September 11 attack, yet, there is still much more to be done by disaster recovery planners.

Chandler and Wallace (2004) found that, the four areas of disaster recovery and business continuity planning areas that were universally recommended for greater attention by both those who already included these dimensions in their plan and those that did not for plan revision, increased focus and modification as: Establishing criteria for resumption of normal operations (define criteria for ending the "declared disaster" phase of operations), Systematic real time tracking of plan implementation, Simulation training for personnel, The planning prioritisation process. In addition, companies that did not include the aspect in the current plans also perceived a need for "significantly" greater attention to the development of a business recovery plan, procedures for plan management, risk assessment, threat identification and crisis team development, organisation, training and assessment.

When preplanning steps are put in place they help prevent utter chaos when a disaster occurs. They are preventative in nature, a thorough process and an attitude shift from the days of false security.

2.2.5 Implementing and Ongoing Management

2.2.5.1 Testing

Testing is important to ensure that there is a reduction on the chaos and confusion that may occur during a disaster. Testing enables the contingency plan to be updated in order to reflect the changes in the environment that affect the organisation. While the nature of the abnormalities the organisation has to contend with may not change over time, the manner in how to respond to them does change (Desouza, 2004).

The DRP must be tested (dry runs) and rehearsed and eventually, a live simulation or scenario of a disaster must be done. This is a technique that better prepares for technology disasters because it affords individuals to get acquainted with distant realities and also provides them with an avenue to test their reflexes and responses to the new environment.

Working with scenarios is critical toward operationalising the plans and seeing how they hold up during times of duress and stress. They can be handled through multiple means, either physical or live demonstrations; they can be simulated using computer technologies and can also be enacted. Regardless of how a scenario is executed, it must meet two goals.

First, scenarios should help reduce the impact of the shock. Shock is the stage immediately following the impact of the crises. It is during the stage of shock where organisations make errors in responding to a crisis. Moreover, the longer the organisation is paralysed after the impact the greater the chance of the crisis escalating.

Second, scenarios should help an individual and organisation calibrate effective and efficient actions after the state of shock. Many times after the initial shock is over, organisations (and individuals) conduct haphazard actions that lead to a worsened situation. Many of these actions will come back to haunt the organisation. Reactionary actions are never wise, unless one has had ample time and opportunity to run through plausible consequences that might be caused due to the actions (Desouza, 2004).

Scenarios must give a sense of reality to the item of interest. The scenario must challenge assumptions. This is the best way to determine weaknesses in the plan, adjust procedures, and modify the roles and responsibilities of departments, support organisations and employees.

2.2.5.2 Training

There is general agreement that, appropriate knowledge and training underpins any organisation's capability to prepare for, respond to, and recover from disasters. Through an ongoing cycle of training, drills, exercises, and tests followed by corrections and enhancements, the organisation's plans and procedures and response capabilities continue to improve (Kildow, 2004).

All employees are responsible for following emergency response and business continuity policies; all employees, not only the designated team members make critical decisions for the organisation every day and will continue doing so in the wake of a disaster. Any plan, or procedure will be of limited value if all employees do not know that it exists, its purpose, and what it means for them (Kildow, 2004). Therefore, it is imperative that, users are made aware of the inherent risks of the information systems they use during the course of doing their jobs and they are more likely to prevent exposures (Maiwald and Sieglein, 2002).

Kildow (2004) further goes on to say that, for assigned team members training must go well beyond handing someone a plan document or checklist of actions and assuming there is complete understanding of the assigned duties. For those involved in carrying out plans, not only must they understand what to do; they should also have a firm understanding of why. Further, an in-depth understanding of how the actions an individual is to take fit in the overall picture, has been shown to the largest factor contributing to employee compliance with established disaster-related policies and preparedness activities prior to an event and ensures following established procedures following a disaster. To ensure that all employees have the necessary knowledge,

establish a comprehensive program that includes education and the necessary level of training for all employees existing and new.

2.2.5.3 Maintenance

Organisations must realise that conditions never remain static in normal business operations. This is an ongoing project, as there are constantly emerging ways that could make organisations vulnerable. Therefore, organisations need to make preparedness a priority and go about in a proactive and thorough way else they will be giving a false cover and jeopardizing their survival (Blythe, 2003).

The planning team therefore, must continually assess the emergency of new threats, adjust for changes in organisational structure and determine the impact of new technology on recovery procedures. Also, depending on the industry, it would be important to monitor changes in the laws and regulations that may affect the disaster recovery requirements.

When procedures are changed and documentation is updated, training requirement and staff skills must be updated as well. Regular reviews help to keep procedures current, and ongoing training ensures that new employees are trained on new or modified procedures.

2.3 IMPORTANCE OF ASPECTS OF DISASTER RECOVERY

It is important and encouraged that, every organisation goes through the process of developing a DRP because at the very least, the process of developing a DRP allows it to identify key assets and to begin planning how it might respond and recovery from a disaster.

Mutunga (2004) says that, a disaster recovery plan enables the setting up of appropriate systems and disaster tolerant infrastructure as well as putting up realistic levels of pre-incident risk reduction initiatives or strategies in order to mitigate disasters or to ensure the fastest possible recovery when faced with disasters.

Communication is key, both to the employees and the stakeholders. Thus, proper communication procedures during planning ensure that organisation's management is proactive in communicating the ongoing status and situation to mitigate the impact of a crisis. This ensures that employees touch base with what is expected of them as well as their responsibilities and the stakeholders are informed of the happenings, thus strengthening existing relationships with all stakeholders as well as attracting new business (Myers, 2003).

DRP process enables the realisation that corporate management must be involved for the plan to be successful. This is because they are responsible for ensuring the resilience of their business operations and have the authority and diligence to work towards the success of the plan (Maiwald and Sieglein, 2002).

The DR team helps co-ordinate the DR management process in order to ensure that the entire organisation is aware about the DR plan and what is expected of them. The awareness thus serves to prepare the whole organisation against a disaster (Maiwald and Sieglein, 2002).

A business impact analysis clarifies the degree of potential loss and unwanted effects while a risk analysis helps determine and prioritise the risks that are most likely to happen within an organisation's environment. Thus, risk reduction measures are put in place in order to avoid the risk, lower the impact of hazards before they strike or to hasten the recovery process (Mutunga 2004).

Risk analysis enables an organisation to evaluate its relationships with interdependent organisations and their value thus plan and establish steps and procedures needed to mitigate a disaster.

Establishing policies and procedures for each department or business unit helps in the co-ordination of activities in order to restore an organisation's functions and business processes (Maiwald and Sieglein, 2002).

In order to fine tune and achieve the best results in the management of disaster recovery, proper training, testing and rehearsal should be considered as the way to go. This enables evaluation of the response in order to determine how well procedures are implemented. It also helps determine weaknesses in the plan, adjustment procedures and modification of the roles and responsibilities for improvement (Desouza, 2004).

Disaster recovery plans and operations could only be feasible if the ultimate users know what their responsibilities are and what is expected of them as well as enable them understand what the organisation is prepared to do in times of disaster. The overall result is a better-prepared organisation and a stronger line of defence against future disaster (Kildow, 2004).

Ongoing management ensures continuous assessment of the plan in order to identify and assess the emergence of new threats, adjustment for changes in organisational structure and determination of the impact of new technology on recovery procedures. It also enables monitoring of changes in the laws and regulations that may affect the disaster recovery requirements.

2.4 CHALLENGES OF EFFECTING A DISASTER RECOVERY PROGRAMME

The attitude of relegating the DR to IT department only without realising that DR requires specific training, tools and equipment across every function of the organisation. This means that the scope and authority of the IT department will be too limited to be effective.

Lack of management understanding that they are responsible for ensuring the resilience of their business operations by realising the challenge is to remain diligent and resolved

towards this by playing roles in the implementation of a disaster recovery management program and by approving and enforcing the program. Some organisations lack internal commitment to disaster recovery management and thus the only driving force is external, for example, customer concerns, or, insurers who push them to guard against business disruption or legal obligations.

The challenge of getting the time and attention of busy managers throughout the organisation to form the disaster recovery team.

The lack of proper evaluation of data in terms of vital, critical and less important data leads to inadequate allocation of capital expenditure and technical expertise thus, poor storage infrastructure and poor availability.

The lack of proper access controls would cost the organisation time, skill and money which management should be willing to fund in order to redesign the controls. This is because information storage may be the most difficult and hardest to appropriately and effectively secure due to much information with different sensitivities, which may be stored together yet different employees may be allowed different levels of access.

Lack of information on the criticality of the systems would lead to inability to identify the cost to the organisation of the loss of the system.

The lack of experience and technical expertise with new technologies among current IT staff due to being overworked and/or overwhelmed by the effort of maintain and troubleshoot an infrastructure that has exceeded its planned capacity due to overdue upgrades or replacement.

Challenge on the technology front for masses to correctly identify the resources necessary to deploy and maintain business continuity which is responsible for ensuring the survivability of our companies and therefore, both the products and the 'experts' should

be selected with care – with validated experience and success being the only appropriate benchmark.

The organisation may spend hundreds of thousands or even millions of dollars on security systems and technologies but a single employee who is unaware of the disaster recovery policies of the organisation can allow an intruder to cause a disaster. This means that, every employee in the organisation must understand the disaster recovery program that has been put in place. This is because authorised users who do not follow the rules may cause some disasters. As with any corporate policy thus, it is important to ensure that every affected employee is made aware of the policy set as pertains to disaster recovery, how to comply and the consequences of non-compliance (Maiwald and Sieglein, 2002).

When organisations fail to track the changes that have occurred in the business/infrastructure/technical environment that they operate in, it results in a lack of realisation that that the plan needs to be reviewed and to develop exercises to validate the plans to ensure that they are still valid.

Lack of identifying and quantifying networked organisation risks inclusive of the threats they pose as well as their values leads to not making them understand the roles and required tasks in order to prepare and work collectively toward resuming normal business operations.

CHAPTER 3: RESEARCH METHODOLOGY

This chapter presented the research design that was used in order to meet the objectives of the study as set out in the introduction.

3.1 Research Design

This research sought to determine the disaster recovery management practises used by companies listed on the NSE and the importance attached to the aspects of disaster recovery. It also sought to establish the challenges faced by these organisations in effecting the disaster recovery programmes. Thus, the researcher had chosen to conduct a survey research. The survey was intended to describe and report the actual happenings within organisations in terms of disaster recovery. It was used to systematically gather factual data from IT managers of the population through questionnaires for decision-making. It was an efficient method of collecting descriptive data regarding aspects of disaster recovery; importance attached to these aspects and the challenges faced by IT managers in effecting disaster recovery programmes.

There is research that has been done on disaster recovery management generally which was not expected to fully explain the aspects of disaster recovery in terms of information technology in companies quoted on the Nairobi Stock Exchange. Thus, the need for this study to identify aspects of disaster recovery in organisations quoted on the NSE, the importance attached to these aspects in view of the unique nature of every business and the challenges faced in effecting disaster recovery. This is in view of the Kenyan social economic and legal context.

3.2 The Population

The population of the study consisted of all firms quoted on the Nairobi Stock Exchange. According to the list of companies listed on the NSE as at 31st July 2004 (Appendix III) the number of firms was forty-eight (48) implying the study population size (N) of 48. This was seen as a small size and given that the firms were within ease of reach a census survey was done. The size and quotation status of companies quoted on the NSE has led

to them having the basic infrastructure and need for information and communication technology based systems and thus, their suitability for this study as they are vulnerable to disasters and are facing crises ever so often. For those firms having several branches, the information required for the study was collected from the head office.

3.3 Data Collection

This study used primary data collected using a questionnaire. The respondents to the study were managers heading the IT departments or their equivalents. In their absence their deputies responded to the questionnaire. These categories of respondents were preferred because they are the ones most familiar and most involved in the information security and recovery issues and so, were able to offer the knowledge sought.

The questionnaire was administered on a "drop and pick-up later" basis for companies within Nairobi and through postal mail with an enclosed self-addressed return envelope for companies outside Nairobi. This method was used to ensure a high proportion of usable responses and a high return rate. There was follow-up to the posted questionnaires through telephone where responses were not prompt.

The questionnaire had four sections with both open and closed questions that were used in tapping information to meet the objectives of the study.

Section A covered the demographic information covering both respondents and organisational profiles.

Section B sought data on aspects of disaster recovery that were considered by the organisations.

Section C was used to collect data on the importance attached to disaster recovery aspects.

Section D collected data on the challenges of effecting disaster recovery plan.

CHAPTER 4: DATA ANALYSIS AND INTERPRETATIONS

4.1 INTRODUCTION

This chapter presents the results of the descriptive analysis of questionnaires from the firms surveyed in this study on aspects of disaster recovery, their importance and the challenges faced in effecting a disaster recovery programme. The data were analysed and resulted in the findings presented in several sections of this chapter.

The final sample of 35 firms was broadly representative of the population of companies quoted on the Nairobi Stock Exchange. The study adopted a census and surveyed 48 of the listed companies. Duly filled questionnaires were received from 35 of them, one (1) was returned without filling with a reason that the company was busy with end year results and 13 were rejected for being incomplete on material items. Thus, the study was based on data on 35 filled questionnaires, which translated to an overall response rate of 77.7%. Considering that indeed most firms were in the annual end year results cycle and the comprehensive nature of the research instrument, this represented a very good response.

4.2 DEMOGRAPHIC CHARACTERISTICS OF THE RESPONDENTS

Demographic factors considered in the study included the types of firms, the position of respondents and the number of years worked in the organisation, the size of firms, the level of information technology use within the organisations, the computerised functions, the position of IT/IS department within the organisational hierarchy, the employees in the IT/IS department, the existence of an IT/IS policy and budget, the level of computer and information literacy within the organisation and the number of employees within the disaster recovery department if any. These factors were to identify the extent of dependency on technology for the information used for decision-making and thus, help identify if organisations should be prepared for business continuity in event of disaster.

4.2.1 Positions of Respondents and Number of Years in the Organisation

Table 4.2.1 represents the positions of the respondents against the number of years they have worked in their organisations. Majority had been working in the organisations for 7 years and above 51%, those that had worked between 4-6 years (22%) and those that had worked for 3-4 years and less than a year at (3%) each. The number of years suggests that due to the length of time in the companies, they had adequate experience in the organisations and thus, their responses could be considered valid and truly reflective of the situation within their organisations, 16 (60%) of them being heads of the Information Technology/Information Systems (IT/IS) departments. Also, the respondents have realised the need to have disaster recovery measures in place in view of the changing status of the environment and their exposures as the organisations have grown in terms of IT exposure and the need to prepare in event of disasters.

Table 4.2.1 Positions of Respondents and Number of Years in the Organisation

Number of years worked in the firm	Total	Title/Position within firm							
		Systems operator	IT Manager	IT Technician	Data assistant	Manager	Clerk	Software support	Accountant
Total	35	1	16	3	1	11	1	1	1
Less than 1yr	3%	0%	6%	0%	0%	0%	0%	0%	0%
1- 2	6%	100%	6%	0%	0%	0%	0%	0%	0%
2- 3	9%	0%	19%	0%	0%	0%	0%	0%	0%
3- 4	3%	0%	6%	0%	0%	0%	0%	0%	0%
4- 5	11%	0%	6%	67%	0%	9%	0%	0%	0%
5- 6	11%	0%	6%	0%	100%	9%	0%	100%	0%
6- 7	17%	0%	19%	33%	0%	18%	0%	0%	0%
7- 8	17%	0%	19%	0%	0%	18%	100%	0%	0%
8- 9	6%	0%	6%	0%	0%	0%	0%	0%	100%
Over 10 yrs	17%	0%	6%	0%	0%	45%	0%	0%	0%

4.2.2 Size of Firms

The size of firms was measured using the number of employees. For the sample, the pattern in Table 4.2.2 emerged. Most of the firms 40% have over 1000 employees with

the agricultural sector having over 2000 employees. This could be attributed to the fact that, they have large plantations or in the manufacturing sector, being companies that use labour intensive methods. Firms with between 101 and 500 employees were next with 31%, those with between 501 and 1000 employees had 23% and the least number of employees were within those organisations that had less than 100 employees and this formed 6%. Therefore, with most organisations having over 100 employees, there is need for them to be aware of the importance of the information they rely on the make business decisions and the need to protect such information.

Table 4.2.2 Size of Firms

	Total	Sector of the organisation				
		Agricultural	Commercial and Services	Finance and Investment	Industrial and Allied	Alternative Investment Market Segment
Total	35	4	11	10	3	7
Less than 100	6%	0%	0%	20%	0%	0%
101-500	31%	0%	45%	20%	33%	43%
501-1000	23%	0%	36%	10%	33%	29%
1001-2000	20%	0%	9%	40%	33%	14%
Over 2001	20%	100%	9%	10%	0%	14%

4.2.3 Level of Information Technology Utilization

Table 4.2.3 represents the level of information technology where 27 (77%) of the companies have a high utilisation of IT. This reflects the realisation of the need for faster and effective processing of information as well as proper storage and backup facilities. The highest usage was within companies in the Commercial and Services sector (31%), closely followed by those in the Finance and Investments sector (29%), Alternative Investment Market Segment (20%), Agricultural sector (11%) and the least being in the Industrial and Allied sector (9%)

Table 4.2.3 Level of Information Technology Utilization

	Total	Level of information technology utilization in the firm		
		High	Average	Low
Total	35	27	7	1
Agricultural	11%	15%	0%	0%
Commercial and Services	31%	26%	43%	100%
Finance and Investment	29%	33%	14%	0%
Industrial and Allied	9%	11%	0%	0%
Alternative Investment Market Segment	20%	15%	43%	0%

4.2.4 Computerised Functions

Table 4.2.4 below shows that most functions are computerised in all the sectors, the payroll processing and supplier base management at 97% in both functions, payments management at 94%, stock ordering and invoicing at 91% for each function, customer base management at 76%, computer aided design at 50% with the least being the other accounting function only 3%. The extensive dependency on information technology infrastructure highlights the increased need to put protection measures to ensure availability of information for business continuity at all times.

Table 4.2.4 Computerised Functions

Computerised functions by sector	Total	Sector of the organisation				
		Agricultural	Commercial and Services	Finance and Investment	Industrial and Allied	Alternative Investment Market Segment
Total	34	4	11	10	3	6
Payroll computerization	97%	100%	100%	90%	100%	100%
Stock ordering computerization	91%	100%	91%	80%	100%	100%
Customer base management computerization	76%	75%	82%	70%	100%	67%
Supplier base management computerization	97%	100%	100%	90%	100%	100%
Payments management computerization	94%	100%	91%	90%	100%	100%
Invoicing computerization	91%	100%	91%	80%	100%	100%
Computer aided design computerization	50%	50%	55%	30%	100%	50%
Accounting computerization	3%	25%	0%	0%	0%	0%

4.2.5 Existence of Information Technology (IT)/Information Systems (IS) Department

Table 4.2.5 shows the existence of information technology (IT)/Information systems (IS) departments within organisations. Only 2 (5.7%) of the companies did not have an IT/IS department probably as this could fall within other departments. Data in table 4.2.5 shows that 33 (94.3%) of the respondent companies have IT/IS departments within their organisations. This would suggest that, companies have realised that information is a fundamental factor of production and thus, the need to invest in information and communications technology.

Table 4.2.5 Existence of Information Technology (IT)/Information Systems (IS) Department

Presence of IT/IS department	Frequency	Percent
Yes	33	94.3
No	2	5.7
Total	35	100.0

4.2.6 Position of IT/IS Department within the Organisation Hierarchy

Table 4.2.6 shows the position of the IT/IS department within the organisational hierarchy. Data in table 4.2.6 shows that 20 (57.1%) of the 35 companies have an independent IT/IS department. 13 (37.1%) of the respondents have the IT/IS department under Finance Department, and 1 each (2.9%) either have the IT/IS function under the Operations Department or Corporate Affairs Department. Having the IT/IS department as an independent department suggests that organisations have realised the need to give this department the scope and authority to carry out its functions. Companies that have placed the IT/IS functions under other departments may pause some conflicts of interest as the IT/IS department has different roles within the organisation.

Table 4.2.6 Position of IT/IS Department within the Organisation Hierarchy

Position of IT/IS department within the organisation hierarchy	Frequency	Percent
Independent	20	57.1
Under Finance	13	37.1
Under Operations Department	1	2.9
Under Corporate Affairs Department	1	2.9
Total	35	100.0

4.2.7 Employees in IT/IS Department

Table 4.2.7 shows the number of employees in the information technology (IT) or information systems (IS) departments across the different sectors. The Finance and Investments sector has the most employees in the IT/IS department 57%. As a percentage of the total, the Commercial and Services sector has most employees in IT/IS department with 33%, the Finance and Investments sector at 27%, the Alternative Investment Market segment at 18% Agricultural sector at 12% and the least being the Industrial and Allied sector at 9%.

Table 4.2.7 Employees in IT/IS Department

Number of people employed in IT or IS within the organisation	Total	Number of people employed in the IT or IS department			
		Less than 10 (IT employees)	10- 20	20- 30	Over 30
Total	33	16	7	3	7
Agricultural	12%	25%	0%	0%	0%
Commercial and Services	33%	44%	14%	0%	43%
Finance and Investment	27%	6%	43%	33%	57%
Industrial and Allied	9%	6%	14%	33%	0%
Alternative Investment Market Segment	18%	19%	29%	33%	0%

4.2.8 Employees Involved in Disaster Recovery

Table 4.2.8 represents the number of employees involved in disaster recovery within the organisations in the different sectors. The Commercial and services sector has most employees involved in disaster recovery (33%), closely followed by finance and investment (30%), the alternative investment market segment (18%), the Agricultural sector (12%) and the least is the industrial and allied sector.

Table 4.2.8 Employees Involved in Disaster Recovery

		Number of employees involved in disaster recovery			
	Total	Less than 10	10- 20	20- 30	Over 30
Total	33	15	12	3	3
Agricultural	12%	27%	0%	0%	0%
Commercial and Services	33%	27%	50%	33%	0%
Finance and Investment	30%	20%	33%	33%	67%
Industrial and Allied	6%	7%	8%	0%	0%
Alternative Investment Market Segment	18%	20%	8%	33%	33%

4.2.9 Existence of an IT/IS Policy

The existence of an IT/IS policy and budget is illustrated in Table 4.2.9. 91% of the respondent organisations have an IT policy. This could be attributed to the fact that, organisations have identified the need to outline what is allowed and what is not to their employees in terms of IT resources in alignment with their business goals and in order to protect their business. 6% of the respondent organisations did not have an IT/IS policy in existence, while 3% were in the process of formulating an IT/IS policy.

Table 4.2.9 Existence of an IT/IS Policy

Existence of IT/IS policy		
Total	34	1
Yes	91%	0%
No	6%	100%
Currently under Formulation	3%	0%

4.2.10 Existence of an IT Budget

From the data in Table 4.2.10, 94% of the respondent organisations have a budget for the IT/IS department, 3% had no budget and the other 3% were in the process of structuring a budget. The need for a budget was attributed to the fact that, the organisations had a strategy and recognised the need to show return on the IT investment as well as seek for funds for future projects.

Table 4.2.10 Existence of an IT Budget

Budget for the IT/IS department		
Total	34	1
Yes	94%	0%
No	3%	100%
Currently under Formulation	3%	0%

4.2.11 Level of Computer and Information Literacy Across Organisational Structure

Table 4.2.10 represents the level of literacy of across different levels of the organisation. The levels of executive director (60%), top management (66%), middle management (53%), and lower management (37%) all have an average level of computer and information literacy. However, the other staff (mainly the subordinates) have a poor understanding of the computer and information literacy (48%). Having an understanding of the need for information across the organisation would enhance the measures put in place to ensure that the information is protected and that it is available at all times.

Table 4.2.11 Level of Computer and Information Literacy Across Organisational Structure

	Poor	%	Average	%	Excellent	%	Total
Executive director	0.0	0.00	21	0.60	14	0.40	35
Top management	1	0.03	23	0.66	11	0.31	35
Mid management	3	0.09	18	0.53	13	0.38	34
Lower management	12	0.34	13	0.37	10	0.29	35
Other	16	0.48	13	0.39	4	0.12	33

4.3 ASPECTS OF DISASTER RECOVERY

4.3.1 Factors Identifying Existence of Aspects of Disaster Recovery

Mean and standard deviations of the aspects of disaster recovery within the respondent organisations were identified. The ratings used were on a scale of 1-5 where 1 was not at all, 3 was moderate and 5 was to a very large extent. Table 4.3.1 lists the aspects of disaster recovery with the means and standard deviations. The aspects that were identified to a large extent amongst the respondent organisations were management being sensitised on the criticality of the information systems and applications they require (4.03), analysing threats and vulnerabilities and prioritising them (4.03) and analysing and prioritising business processes (4.03). Also, having a disaster recovery plan, which documents the procedures during a disaster event, was an aspect that scored a mean of 4.0. The above identify the following three major aspects of disaster recovery: firstly, management support, secondly risk analysis and business impact analysis and thirdly, having contingency plans and procedures in place. All other aspects had a moderate mean rate including having a disaster recovery team, testing, training and maintenance.

It can be deduced, therefore, that, organisations have realised the need for management to be involved in disaster recovery preparedness as they must approve the disaster recovery plan, enforce the policy, help develop and approve the written plan, help ensure that the employees understand the plan and they must also participate in following the procedures for each policy and enforce the policies where necessary.

The aspect of having a disaster recovery plan was identified by most respondent organisations and this would enable them carry out impact analysis to identify critical systems and data and the impact an outage would have on business continuity, carry out a risk analysis to identify threats and vulnerabilities, and evaluate the measures in place to counter the threats and vulnerabilities, allocate funds for disaster recovery preparedness, outline procedures in event of a disaster, involve employees in understanding laid out policies and train them for preparation in event of a disaster, carry out regular testing of the plain to enable updating and having a current plan.

Table 4.3.1 Factors Identifying Existence of Aspects of Disaster Recovery

	Mean	Std. Deviation
Management is sensitised on the criticality of the information systems and applications required	4.03	0.797
The importance of supporting disaster recovery plan for success is recognized by the management	3.94	0.851
Priorities for recovery in the event of disaster have been laid out	3.71	1.142
The organisation's philosophy for disaster recovery is clearly articulated by management	3.56	1.021
The organisation's finance and time availability are taken into consideration during disaster recovery planning	3.91	0.866
Goals for recovery and restoration of business have been outlined	3.91	1.164
The disaster recovery team provides leadership on necessary actions in the event of a disaster	3.85	1.132
There are policies and procedures governing communication to all stakeholders and media	3.56	1.133
There is a disaster recovery team in the organisation	3.50	1.135
There is a recovery department that deals with disaster recovery issues	3.18	1.466
The disaster recovery team is composed of appropriate individuals in terms of leadership, skills and trustworthiness	3.59	1.395
The disaster recovery team includes members from all business units	3.21	1.321
Members of the disaster recovery team have specific job descriptions	3.26	1.377
The need for budget for disaster recovery planning is recognised by management	3.76	1.257
There are laid out alternatives and replacements in terms of resource and systems in the event of a disaster	3.82	1.242
Key personnel within the organisation are involved in identifying business critical areas	3.88	1.122
Threats and vulnerabilities facing the organisation has analysed and categorised its risks	4.03	1.167
Measures have been put in place to reduce identified risks	3.88	1.175
The business processes have been analysed and prioritised in terms of criticality	4.03	1.193
Procedures are laid out on determining if an event is a disaster or not and action to be taken	3.79	1.122
The business has identified the impact to its operations if certain external groups failed to execute required functions	3.74	1.163
There is legal counsel within the organisation to offer	3.65	1.098

	Mean	Std. Deviation
component legal advise		
There are manual processes in place to support overall business objectives in event of a disaster	3.50	1.052
There exists a disaster recovery plan	3.62	0.985
The documents that helped publish the disaster recovery plan are available	3.71	1.244
There exists procedures for communicating with employees during response and recovery after a disaster event	3.50	1.161
There exists disaster recovery procedures that relate to direction, control and administration	3.74	1.082
Departments have formal procedures stipulating what is to be done in the event of a disaster	3.74	1.109
Inventory in terms of all assets of the organisation are held	3.74	1.136
The disaster recovery plan documents the steps to be taken during a disaster	4.00	1.044
There is constant testing of the disaster recovery plan in different scenarios	3.76	1.257
Employees are involved in testing the disaster recovery plan	3.18	1.141
There are clear roles and responsibilities for disaster recovery plan	3.24	1.075
There exists an awareness campaign to inform employees on the ongoing disaster recovery planning efforts	3.24	1.103
Employees are involved in training programmes	3.26	1.109
The disaster recovery team members have a checklist of actions to help them understand their duties	3.32	1.147
There is constant drilling and training of the disaster recovery team on the procedures	3.24	1.415
There exist procedures on restoring facilities and normalizing operations after a disaster	3.41	1.234
There are constant reviews and updating of the disaster recovery plan	3.50	1.212
There exists an insurance policy for the assets that could be affected in case of a disaster	3.53	1.212
The information technology department has processes in place to ease recovery of damaged computer systems	3.71	1.244
There is constant evaluation of laws and regulations to ensure compliance	3.82	1.218
Audits are often carried out as a risk management tool	3.53	1.187

4.4 IMPORTANCE OF ASPECTS OF DISASTER RECOVERY

4.4.1 List of Factors Identifying the Importance of Aspects of Disaster Recovery

Factor analysis was performed on the results of the importance attached to the different aspects of disaster recovery. Factor analysis is a technique applicable where there is a systematic interdependence among a set of observed or manifested variable and the researcher is interested in finding out something more fundamental or latent which creates commonality. Thus factor analysis seeks to resolve a large set of measured variables in terms of relatively few categories, known as factors. The factors are listed in Table 4.4.1.

Table 4.4.1 List of Factors Identifying the Importance of Aspects of Disaster Recovery

1	Management support
2	Identification of the criticality of the information system and application
3	Clearly laid out recovery and restoration
4	Proper communication procedures for stakeholders and media
5	Existence of a disaster recovery team
6	Autonomy and authority for disaster recovery team
7	A department dealing with disaster recovery issues
8	Specific job descriptions for members of the disaster recovery team
9	Alternatives and replacements for infrastructure and resources
10	Procedures on handling external independent groups
11	Identification of risks, vulnerabilities and exposures
12	Measures for dealing with risks, vulnerabilities and exposures
13	Identification of key disaster recovery procedures and processes
14	Involvement of all business units in disaster recovery planning issues
15	Technological expertise and experience of the disaster recovery planning
16	Proper budgeting and financing for disaster recovery planning
17	Legal department to offer legal counsel
18	Existence of a disaster recovery plan
19	Training employees on disaster recovery (user awareness and education)
20	Employees involved in testing the disaster recovery plan
21	Constant review and updating the disaster recovery plan
22	Alternative manual processes
23	Insurance related policies or coverage in event of a disaster have been effected
24	Insurance policy in event of disaster
25	Procedures for communicating with employees in event of a disaster
26	Inventory of organisations asset is available
27	Constant drilling and training of the disaster recovery team members
28	Evaluation of laws and regulations for compliance
29	Audit for risk management

4.4.2 Correlation Matrix for Identifying Importance Attached to Aspects of Disaster Recovery

Each respondent indicated the level of importance attached to the different aspects of disaster recovery. The extraction method was the primary component analysis. The coefficients of correlation express the degree of linear relationship between the row and column variables of the matrix. A weak relationship exists the closer to zero the coefficient, while the closer to one, the stronger the relationship. A negative sign indicates that the variables are inversely related. From the correlation matrix, Table 4.4.2 indicates the correlation coefficients are more close to one meaning that there is a relationship between the variables.

Table 4.4.2 Correlation Matrix for Identifying Importance Attached to Aspects of Disaster Recovery

Component	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1.00	0.88	0.73	0.57	0.58	0.48	0.27	0.49	0.75	0.70	0.73	0.73	0.65	0.58	0.39
2	0.88	1.00	0.89	0.62	0.61	0.60	0.42	0.50	0.79	0.73	0.78	0.83	0.75	0.62	0.46
3	0.73	0.89	1.00	0.46	0.56	0.54	0.38	0.43	0.60	0.62	0.64	0.66	0.63	0.50	0.57
4	0.57	0.62	0.46	1.00	0.72	0.81	0.70	0.72	0.53	0.41	0.49	0.55	0.61	0.71	0.47
5	0.58	0.61	0.56	0.72	1.00	0.91	0.78	0.90	0.63	0.42	0.57	0.62	0.76	0.74	0.67
6	0.48	0.60	0.54	0.81	0.91	1.00	0.86	0.90	0.62	0.42	0.57	0.64	0.78	0.74	0.64
7	0.27	0.42	0.38	0.70	0.78	0.86	1.00	0.83	0.41	0.26	0.39	0.48	0.66	0.68	0.65
8	0.49	0.50	0.43	0.72	0.90	0.90	0.83	1.00	0.54	0.31	0.50	0.54	0.74	0.72	0.65
9	0.75	0.79	0.60	0.53	0.63	0.62	0.41	0.54	1.00	0.82	0.94	0.89	0.81	0.71	0.41
10	0.70	0.73	0.62	0.41	0.42	0.42	0.26	0.31	0.82	1.00	0.91	0.82	0.72	0.64	0.41
11	0.73	0.78	0.64	0.49	0.57	0.57	0.39	0.50	0.94	0.91	1.00	0.92	0.83	0.70	0.48
12	0.73	0.83	0.66	0.55	0.62	0.64	0.48	0.54	0.89	0.82	0.92	1.00	0.90	0.69	0.52
13	0.65	0.75	0.63	0.61	0.76	0.78	0.66	0.74	0.81	0.72	0.83	0.90	1.00	0.79	0.69
14	0.58	0.62	0.50	0.71	0.74	0.74	0.68	0.72	0.71	0.64	0.70	0.69	0.79	1.00	0.65
15	0.39	0.46	0.57	0.47	0.67	0.64	0.65	0.65	0.41	0.41	0.48	0.52	0.69	0.65	1.00
16	0.65	0.74	0.61	0.58	0.56	0.62	0.47	0.55	0.81	0.73	0.83	0.84	0.84	0.68	0.48
17	0.58	0.69	0.48	0.52	0.55	0.60	0.50	0.60	0.80	0.65	0.77	0.81	0.82	0.69	0.44
18	0.76	0.77	0.59	0.55	0.74	0.69	0.51	0.71	0.87	0.65	0.80	0.85	0.86	0.70	0.55
19	0.63	0.64	0.44	0.74	0.64	0.70	0.53	0.67	0.76	0.59	0.69	0.70	0.73	0.77	0.53
20	0.70	0.67	0.48	0.77	0.80	0.79	0.66	0.78	0.75	0.59	0.69	0.74	0.79	0.83	0.60
21	0.64	0.68	0.56	0.59	0.70	0.73	0.57	0.70	0.81	0.66	0.78	0.81	0.85	0.77	0.64
22	0.69	0.75	0.70	0.48	0.52	0.54	0.38	0.49	0.74	0.77	0.78	0.77	0.77	0.58	0.39
23	0.53	0.67	0.68	0.48	0.35	0.43	0.25	0.21	0.44	0.42	0.43	0.50	0.39	0.18	0.13
24	0.64	0.78	0.80	0.44	0.37	0.45	0.24	0.28	0.55	0.53	0.55	0.63	0.51	0.27	0.23
25	0.71	0.80	0.60	0.70	0.68	0.73	0.55	0.62	0.83	0.56	0.72	0.81	0.73	0.66	0.46
26	0.72	0.77	0.84	0.33	0.32	0.34	0.11	0.17	0.59	0.66	0.62	0.62	0.48	0.32	0.31
27	0.56	0.56	0.38	0.69	0.57	0.67	0.57	0.64	0.65	0.51	0.61	0.69	0.69	0.72	0.55
28	0.71	0.74	0.55	0.49	0.57	0.59	0.43	0.55	0.86	0.72	0.83	0.83	0.79	0.67	0.42
29	0.71	0.75	0.59	0.56	0.60	0.62	0.47	0.57	0.86	0.73	0.84	0.81	0.79	0.73	0.48

Component	16	17	18	19	20	21	22	23	24	25	26	27	28	29
1	0.65	0.58	0.76	0.63	0.70	0.64	0.69	0.53	0.64	0.71	0.72	0.56	0.71	0.71
2	0.74	0.69	0.77	0.64	0.67	0.68	0.75	0.67	0.78	0.80	0.77	0.56	0.74	0.75
3	0.61	0.48	0.59	0.44	0.48	0.56	0.70	0.68	0.80	0.60	0.84	0.38	0.55	0.59
4	0.58	0.52	0.55	0.74	0.77	0.59	0.48	0.48	0.44	0.70	0.33	0.69	0.49	0.56
5	0.56	0.55	0.74	0.64	0.80	0.70	0.52	0.35	0.37	0.68	0.32	0.57	0.57	0.60
6	0.62	0.60	0.69	0.70	0.79	0.73	0.54	0.43	0.45	0.73	0.34	0.67	0.59	0.62
7	0.47	0.50	0.51	0.53	0.66	0.57	0.38	0.25	0.24	0.55	0.11	0.57	0.43	0.47
8	0.55	0.60	0.71	0.67	0.78	0.70	0.49	0.21	0.28	0.62	0.17	0.64	0.55	0.57
9	0.81	0.80	0.87	0.76	0.75	0.81	0.74	0.44	0.55	0.83	0.59	0.65	0.86	0.86
10	0.73	0.65	0.65	0.59	0.59	0.66	0.77	0.42	0.53	0.56	0.66	0.51	0.72	0.73
11	0.83	0.77	0.80	0.69	0.69	0.78	0.78	0.43	0.55	0.72	0.62	0.61	0.83	0.84
12	0.84	0.81	0.85	0.70	0.74	0.81	0.77	0.50	0.63	0.81	0.62	0.69	0.83	0.81
13	0.84	0.82	0.86	0.73	0.79	0.85	0.77	0.39	0.51	0.73	0.48	0.69	0.79	0.79
14	0.68	0.69	0.70	0.77	0.83	0.77	0.58	0.18	0.27	0.66	0.32	0.72	0.67	0.73
15	0.48	0.44	0.55	0.53	0.60	0.64	0.39	0.13	0.23	0.46	0.31	0.55	0.42	0.48
16	1.00	0.84	0.79	0.75	0.73	0.84	0.84	0.56	0.63	0.76	0.64	0.72	0.86	0.89
17	0.84	1.00	0.87	0.73	0.71	0.81	0.67	0.28	0.47	0.80	0.44	0.76	0.85	0.83
18	0.79	0.87	1.00	0.78	0.82	0.88	0.73	0.36	0.53	0.84	0.53	0.73	0.87	0.85
19	0.75	0.73	0.78	1.00	0.92	0.91	0.67	0.28	0.37	0.81	0.43	0.90	0.81	0.83
20	0.73	0.71	0.82	0.92	1.00	0.89	0.65	0.27	0.35	0.81	0.41	0.88	0.79	0.80
21	0.84	0.81	0.88	0.91	0.89	1.00	0.78	0.32	0.45	0.82	0.54	0.87	0.89	0.90
22	0.84	0.67	0.73	0.67	0.65	0.78	1.00	0.61	0.72	0.62	0.76	0.57	0.80	0.81
23	0.56	0.28	0.36	0.28	0.27	0.32	0.61	1.00	0.92	0.53	0.77	0.23	0.43	0.44
24	0.63	0.47	0.53	0.37	0.35	0.45	0.72	0.92	1.00	0.64	0.88	0.37	0.58	0.56
25	0.76	0.80	0.84	0.81	0.81	0.82	0.62	0.53	0.64	1.00	0.61	0.84	0.86	0.84
26	0.64	0.44	0.53	0.43	0.41	0.54	0.76	0.77	0.88	0.61	1.00	0.43	0.65	0.66
27	0.72	0.76	0.73	0.90	0.88	0.87	0.57	0.23	0.37	0.84	0.43	1.00	0.81	0.79
28	0.86	0.85	0.87	0.81	0.79	0.89	0.80	0.43	0.58	0.86	0.65	0.81	1.00	0.96
29	0.89	0.83	0.85	0.83	0.80	0.90	0.81	0.44	0.56	0.84	0.66	0.79	0.96	1.00

4.4.3 Total Variance Explained for Identifying Importance Attached to the Difference Aspects of Disaster Recovery

Table 4.4.3 shows all the factors extracted from the analysis along with their Eigen values, the percentages of variance attributed to each factor and cumulative variance of the factor and previous factors. The first 4 factors were the only ones with Eigen values greater than 1. The first factor, management support accounts for 66.2%, the second, identification of criticality of the information system and application accounts for 10.9%, the third, clearly laid out procedures for restoration and recovery, accounts for 6.1%, and the fourth, proper communication procedures for stakeholders and media, accounts for 3.4% of the variance. This shows that these 4 have the highest importance attached to them by the respondents.

Table 4.4.3 Total Variance Explained for Identifying Importance Attached to the Difference Aspects of Disaster Recovery

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	19.213	66.253	66.253	19.213	66.253	66.253	10.76	37.102	37.102
2	3.164	10.91	77.163	3.164	10.91	77.163	7.066	24.367	61.469
3	1.797	6.195	83.358	1.797	6.195	83.358	5.998	20.681	82.15
4	1.005	3.464	86.822	1.005	3.464	86.822	1.355	4.672	86.822
5	0.673	2.319	89.141						
6	0.632	2.179	91.321						
7	0.544	1.875	93.195						
8	0.403	1.39	94.585						
9	0.288	0.991	95.577						
10	0.242	0.834	96.411						
11	0.178	0.615	97.026						
12	0.158	0.546	97.572						
13	0.143	0.492	98.064						
14	0.121	0.417	98.48						
15	0.092	0.316	98.797						
16	0.082	0.282	99.078						
17	0.067	0.231	99.309						
18	0.05	0.171	99.48						
19	0.04	0.137	99.618						
20	0.035	0.119	99.737						
21	0.029	0.099	99.835						
22	0.019	0.064	99.899						
23	0.014	0.047	99.946						
24	0.007	0.023	99.969						
25	0.005	0.018	99.987						
26	0.002	0.008	99.996						
27	0.001	0.004	99.999						
28	0	0.001	100						
29	0	0	100						
Extraction Method: Principal Component Analysis.									

4.4.4 Component Matrix for Identifying Importance of Different Aspects of Disaster Recovery

Once the factors are extracted, it is possible to calculate the loading of the importance on each factor. The higher the absolute value of the loading, the more the importance that is attached to the factor. Table 4.4.5 represents the component matrix for identifying the importance attached to different aspects of disaster recovery.

Table 4.4.4 Component Matrix for Identifying Importance of Different Aspects of Disaster Recovery

	Component			
	1	2	3	4
Management support	0.799	0.28	0.04	0.027
Identification of the criticality of the information system and application	0.868	0.32	0.17	0.053
Clearly laid out recovery and restoration	0.732	0.38	0.39	0.251
Proper communication procedures for stakeholders and media	0.728	-0.29	0.34	-0.29
Existence of a disaster recovery team	0.782	-0.38	0.33	0.115
Autonomy and authority for disaster recovery team	0.803	-0.39	0.36	-0.04
A department dealing with disaster recovery issues	0.63	-0.55	0.37	0.047
Specific job descriptions for members of the disaster recovery team	0.735	-0.53	0.26	0.026
Alternatives and replacements for infrastructure and resources	0.895	0.13	-0.24	0.068
Procedures on handling external independent groups	0.771	0.31	-0.25	0.307
Identification of risks, vulnerabilities and exposures	0.876	0.18	-0.24	0.241
Measures for dealing with risks, vulnerabilities and exposures	0.907	0.14	-0.13	0.138
Identification of key disaster recovery procedures and processes	0.914	-0.12	-0.03	0.238
Involvement of all business units in disaster recovery planning issues	0.816	-0.34	-0.06	0.153
Technological expertise and experience of the disaster recovery planning	0.626	-0.35	0.2	0.429
Proper budgeting and financing for disaster recovery planning	0.892	0.14	-0.14	-0.05
Legal department to offer legal counsel	0.844	-0.06	-0.3	-0.05
Existence of a disaster recovery plan	0.911	-0.05	-0.16	0.03
Training employees on disaster recovery (user awareness and education)	0.858	-0.23	-0.2	-0.25
Employees involved in testing the disaster recovery plan	0.886	-0.31	-0.08	-0.13
Constant review and updating the disaster recovery plan	0.919	-0.15	-0.2	-0.04
Alternative manual processes	0.835	0.3	-0.03	0.049
Insurance related policies or coverage in event of a disaster have been effected	0.539	0.56	0.51	-0.23
Insurance policy in event of disaster	0.656	0.59	0.37	-0.15
Procedures for communicating with employees in event of a disaster	0.895	0	-0.01	-0.31
Inventory of organisations asset is available	0.671	0.64	0.16	-0.04
Constant drilling and training of the disaster recovery team members	0.815	-0.27	-0.2	-0.33
Evaluation of laws and regulations for compliance	0.901	0.11	-0.29	-0.14
Audit for risk management	0.915	0.08	-0.25	-0.1
Extraction Method: Principal Component Analysis.				

4.4.5 Rotated Component Matrix for Identifying the Importance Attached to the Different Aspects of Disaster Recovery

Factor rotation was done to reduce the number of factors on which the variables under investigation had high loadings. The gaps on the Table 4.4.6 represent loadings that are less than 0.4.

Table 4.4.5 Rotated Component Matrix for Identifying the Importance Attached to the Different Aspects of Disaster Recovery

	Component			
	1	2	3	4
Management support	0.547		0.579	
Identification of the criticality of the information system and application	0.509		0.701	
Clearly laid out recovery and restoration			0.784	
Proper communication procedures for stakeholders and media		0.732		
Existence of a disaster recovery team		0.838		
Autonomy and authority for disaster recovery team		0.866		
A department dealing with disaster recovery issues		0.895		
Specific job descriptions for members of the disaster recovery team		0.873		
Alternatives and replacements for infrastructure and resources	0.794			
Procedures on handling external independent groups	0.680		0.413	0.456
Identification of risks, vulnerabilities and exposures	0.755			
Measures for dealing with risks, vulnerabilities and exposures	0.720		0.429	
Identification of key disaster recovery procedures and processes	0.637	0.546		
Involvement of all business units in disaster recovery planning issues	0.594	0.631		
Technological expertise and experience of the disaster recovery planning		0.687		0.454
Proper budgeting and financing for disaster recovery planning	0.746		0.428	
Legal department to offer legal counsel	0.817			
Existence of a disaster recovery plan	0.758	0.422		
Training employees on disaster recovery (user awareness and education)	0.785	0.487		
Employees involved in testing the disaster recovery plan	0.701	0.626		
Constant review and updating the disaster recovery plan	0.799	0.471		
Alternative manual processes	0.621		0.572	
Insurance related policies or coverage in event of a disaster have been effected			0.928	
Insurance policy in event of disaster			0.929	
Procedures for communicating with employees in event of a disaster	0.696	0.444	0.424	
Inventory of organisations asset is available			0.853	
Constant drilling and training of the disaster recovery team members	0.765	0.486		
Evaluation of laws and regulations for compliance	0.867			
Audit for risk management	0.842			

Variables (aspects) that load heavily towards component 1 are:

a) Alternatives and replacements for infrastructure and resources;

b) Procedures on handling external independent groups;

c) Identification of risks, vulnerabilities and exposures;

d) Measures for dealing with risks, vulnerabilities and exposures;

e) Identification of key disaster recovery procedures and processes;

f) Proper budgeting and financing for disaster recovery planning;

g) Legal department to offer legal counsel;

h) Existence of a disaster recovery plan;

i) Training employees on disaster recovery (user awareness and education);

j) Employees involved in testing the disaster recovery plan;

k) Constant review and updating the disaster recovery plan;

l) Alternative manual processes;

m) Procedures for communicating with employees in event of a disaster;

n) Inventory of organisations asset is available;

o) Constant drilling and training of the disaster recovery team members;

p) Evaluation of laws and regulations for compliance; and

q) Audit for risk management.

The major aspects identified above are business impact and risk analysis, implementing and ongoing management, having a disaster recovery plan.

Variables (aspects) that load heavily towards component 2 are:

a) Involvement of all business units in disaster recovery planning issues; and

b) Technological expertise and experience of the disaster recovery planning

The major aspect identified above is having a disaster recovery plan.

Variables (aspects) that load heavily towards component 3 are:

a) Management support;

b) Identification of the criticality of the information system and application;

c) Clearly laid out recovery and restoration;

d) Insurance related policies or coverage in event of a disaster have been effected; and

e) Insurance policy in event of disaster.

The aspects identified above are management support, business impact analysis and having a disaster recovery plan.

4.5 CHALLENGES IN IMPLEMENTING DISASTER RECOVERY

4.5.1 Factors Identifying Challenges of Implementing Disaster Recovery Programmes

The results from the respondents on the challenges of effecting disaster recovery programmes were analysed using factor analysis. Section 4.4 highlights the purpose of factor analysis and it has been used to resolve a large set of measured variables in terms of relatively few categories or factors. The factors are listed in Table 4.5.1 with their means and standard deviations.

Table 4.5.1 Factors Identifying Challenges of Implementing Disaster Recovery Programmes

	Mean	Std. Deviation
The scope and authority of disaster recovery issues is limited to the IT or IS departments only	3.23	1.087
Management does not support disaster recovery issues	3.94	1.027
There is no information on the criticality of the systems and applications	3.80	0.964
There is no quantification of the cost of unavailability of systems	3.51	1.222
There are insufficient funds to support the implementation of a disaster recovery programme	3.60	1.117
There is lack of awareness among employees on the existence of a disaster recovery plan	3.49	1.147
There is lack of internal commitment to disaster recovery	3.63	1.031
There is no protection of data and information	3.89	1.132
There is no proper design of the storage system for purposes of backup	4.11	0.932
There lacks proper documentation of procedures and processes	3.86	0.944
There lacks skills and expertise amongst the disaster recovery team	3.97	0.891
Employees are not trained on what to do in event of a disaster	3.43	1.145
There is no testing of the disaster recovery plan	3.51	1.245
The organisation structure does not cater for a disaster recovery department	3.34	1.211
The impact of a disaster on the survivability of the business has not been identified	3.57	1.119
There is lack of proper coordination of the disaster recovery programme	3.51	1.067
There is a lack of proper mechanisms to facilitate reviews of the disaster recovery plan	3.34	1.187

4.5.2 Correlation Matrix for Identifying Challenges of Effecting Disaster Recovery Programmes

Respondents indicated their agreement degrees on the challenges of implementing disaster recovery programmes. The extraction method was the primary component analysis. A weak relationship exists the closer to zero the coefficient, while the closer to one, the stronger the relationship. A negative sign indicates that the variables are inversely related. The correlation matrix as represented in Table 4.5.2 presents a highly positively correlation between variables thus showing a relationship between them.

Table 4.5.2 Correlation Matrix for Identifying Challenges of Effecting Disaster Recovery Programmes

Component	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	1.000	0.381	0.382	0.352	0.683	0.663	0.393	0.333	0.235	0.348	0.372	0.675	0.649	0.363	0.397	0.327	0.439
2	0.381	1.000	0.938	0.633	0.518	0.598	0.729	0.728	0.867	0.719	0.705	0.597	0.713	0.465	0.592	0.484	0.547
3	0.382	0.938	1.000	0.589	0.525	0.596	0.692	0.652	0.812	0.711	0.712	0.560	0.725	0.438	0.627	0.474	0.447
4	0.352	0.633	0.589	1.000	0.328	0.614	0.436	0.299	0.515	0.627	0.392	0.532	0.556	0.732	0.575	0.355	0.504
5	0.683	0.518	0.525	0.328	1.000	0.753	0.531	0.265	0.271	0.279	0.550	0.667	0.871	0.561	0.753	0.548	0.462
6	0.663	0.598	0.596	0.614	0.753	1.000	0.704	0.407	0.387	0.609	0.647	0.733	0.849	0.766	0.786	0.511	0.522
7	0.393	0.729	0.692	0.436	0.531	0.704	1.000	0.593	0.627	0.639	0.724	0.687	0.680	0.529	0.623	0.633	0.636
8	0.333	0.728	0.652	0.299	0.265	0.407	0.593	1.000	0.710	0.480	0.464	0.538	0.419	0.244	0.401	0.294	0.359
9	0.235	0.867	0.812	0.515	0.271	0.387	0.627	0.710	1.000	0.755	0.642	0.421	0.480	0.251	0.359	0.383	0.442
10	0.348	0.719	0.711	0.627	0.279	0.609	0.639	0.480	0.755	1.000	0.800	0.467	0.515	0.430	0.386	0.309	0.439
11	0.372	0.705	0.712	0.392	0.550	0.647	0.724	0.464	0.642	0.800	1.000	0.474	0.597	0.418	0.489	0.480	0.399
12	0.675	0.597	0.560	0.532	0.667	0.733	0.687	0.538	0.421	0.467	0.474	1.000	0.769	0.612	0.676	0.440	0.560
13	0.649	0.713	0.725	0.556	0.871	0.849	0.680	0.419	0.480	0.515	0.597	0.769	1.000	0.640	0.796	0.547	0.633
14	0.363	0.465	0.438	0.732	0.561	0.766	0.529	0.244	0.251	0.430	0.418	0.612	0.640	1.000	0.828	0.451	0.448
15	0.397	0.592	0.627	0.575	0.753	0.786	0.623	0.401	0.359	0.386	0.489	0.676	0.796	0.828	1.000	0.510	0.380
16	0.327	0.484	0.474	0.355	0.548	0.511	0.633	0.294	0.383	0.309	0.480	0.440	0.547	0.451	0.510	1.000	0.762
17	0.439	0.547	0.447	0.504	0.462	0.522	0.636	0.359	0.442	0.439	0.399	0.560	0.633	0.448	0.380	0.762	1.000

4.5.3 Total Variance Explained for Identifying Challenges of Effecting Disaster Recovery Programmes

Table 4.5.3 shows all the components extracted from the analysis along with their Eigen values, the percentages of variance attributed to each component and cumulative variance of the factor and previous factors. The first 3 factors were the only ones with Eigen values greater than 1. The first factor, the scope and authority of disaster recovery issues is limited to the IT/IS departments only accounts for 58.1%, the second, management does not support disaster recovery issues, accounts for 11.6%, and the third, there is no

information on the criticality of the systems and applications, accounts for 6.2% of the variance. These show that these three are the greatest challenges to implementing disaster recovery programmes.

Table 4.5.3 Total Variance Explained for Identifying Challenges of Effecting Disaster Recovery Programmes

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	9.889	58.169	58.169	9.889	58.169	58.169	5.056	29.743	29.743
2	1.987	11.686	69.855	1.987	11.686	69.855	4.444	26.142	55.884
3	1.069	6.291	76.145	1.069	6.291	76.145	3.444	20.261	76.145
4	0.986	5.799	81.945						
5	0.743	4.371	86.316						
6	0.718	4.222	90.538						
7	0.511	3.005	93.543						
8	0.277	1.63	95.172						
9	0.193	1.138	96.31						
10	0.163	0.958	97.268						
11	0.127	0.748	98.016						
12	0.116	0.681	98.697						
13	0.087	0.509	99.206						
14	0.061	0.356	99.563						
15	0.036	0.215	99.777						
16	0.022	0.131	99.908						
17	0.016	0.092	100						

Extraction Method: Principal Component Analysis.

4.5.4 Component Matrix for Identifying Challenges of Effecting Disaster Recovery Programmes

Once the factors are extracted, it is possible to calculate the loading of the challenges on each factor. The higher the absolute value of the loading the more the challenge contributes to the factor. Table 4.5.4 shows that only 3 factors have been extracted. The gaps on the table represent loadings that are less than 0.4, thus making it easier to read the table.

Table 4.5.4 Component Matrix for Identifying Challenges of Effecting Disaster Recovery Programmes

	Component		
	1	2	3
The scope and authority of disaster recovery issues is limited to the IT or IS departments only	0.613		
Management does not support disaster recovery issues	0.872		
There is no information on the criticality of the systems and applications	0.849		
There is no quantification of the cost of unavailability of systems	0.699		
There are insufficient funds to support the implementation of a disaster recovery programme	0.745		
There is lack of awareness among employees on the existence of a disaster recovery plan	0.867		
There is lack of internal commitment to disaster recovery	0.844		
There is no protection of data and information	0.631	0.440	
There is no proper design of the storage system for purposes of backup	0.709	0.628	
There lacks proper documentation of procedures and processes	0.738	0.427	
There lacks skills and expertise amongst the disaster recovery team	0.769		
Employees are not trained on what to do in event of a disaster	0.807		
There is no testing of the disaster recovery plan	0.892		
The organisation structure does not cater for a disaster recovery department	0.713		
The impact of a disaster on the survivability of the business has not been identified	0.795		
There is lack of proper coordination of the disaster recovery programme	0.653		0.411
There is a lack of proper mechanisms to facilitate reviews of the disaster recovery plan	0.688		

4.5.5 Rotated Component Matrix for Identifying Challenges of Effecting Disaster Recovery Programmes

Factor rotation is done to reduce the number of factors on which the variables under investigation have high loadings. This does not change anything but makes the interpretation of the analysed data easier. The gaps on the table represent loadings that are less that 0.4, thus making it easier to read the table. From the rotated matrix in Table 4.5.5, it can be seen that:

Variables (challenges) that load heavily towards component 1 are:

a) Management does not support disaster recovery issues;

b) There is no information on the criticality of the systems and applications;

c) There is lack of internal commitment to disaster recovery;

d) There is no protection of data and information;

e) There is no proper design of the storage system for purposes of backup;

f) There lacks proper documentation of procedures and processes; and

g) There lacks skills and expertise amongst the disaster recovery team.

The challenges are on lack of management support, lack of business impact analysis being carried out and the lack of a disaster recovery plan

Variables (challenges) that load heavily towards component 2 are:

a) The scope and authority of disaster recovery issues is limited to the IT or IS departments only;

b) There are insufficient funds to support the implementation of a disaster recovery programme;

c) Employees are not trained on what to do in event of a disaster;

d) There is no testing of the disaster recovery plan;

e) There is lack of proper coordination of the disaster recovery programme; and

f) There is a lack of proper mechanisms to facilitate reviews of the disaster recovery plan.

The main challenges are lack of a disaster recovery plan and lack of maintenance.

Variables (challenges) that load heavily towards component 3 are:

a) There is no quantification of the cost of unavailability of systems;

b) There is lack of awareness among employees on the existence of a disaster recovery plan;

c) The organisation structure does not cater for a disaster recovery department; and

d) The impact of a disaster on the survivability of the business has not been identified.

There lacks management support and lack of carrying out of the business impact analysis.

Table 4.5.5 Rotated Component Matrix for Identifying Challenges of Effecting Disaster Recovery Programmes

	Component		
	1	2	3
The scope and authority of disaster recovery issues is limited to the IT or IS departments only		0.698	
Management does not support disaster recovery issues	0.841		
There is no information on the criticality of the systems and applications	0.800		
There is no quantification of the cost of unavailability of systems	0.426		0.752
There are insufficient funds to support the implementation of a disaster recovery programme		0.799	0.408
There is lack of awareness among employees on the existence of a disaster recovery plan		0.591	0.653
There is lack of internal commitment to disaster recovery	0.625	0.558	
There is no protection of data and information	0.741		
There is no proper design of the storage system for purposes of backup	0.933		
There lacks proper documentation of procedures and processes	0.788		
There lacks skills and expertise amongst the disaster recovery team	0.683		
Employees are not trained on what to do in event of a disaster		0.641	0.448
There is no testing of the disaster recovery plan		0.705	0.507
The organisation structure does not cater for a disaster recovery department			0.858
The impact of a disaster on the survivability of the business has not been identified		0.483	0.722
There is lack of proper coordination of the disaster recovery programme		0.721	
There is a lack of proper mechanisms to facilitate reviews of the disaster recovery plan		0.682	

Extraction Method: Principal Component Analysis.

4.6 RECOMMENDATIONS

It is acknowledged that there is growing dependence of IT computer based information systems. This means that, the data they hold and the ability to process the same constitutes a major corporate asset. Therefore, anything denying access to this continuity of business in a timely and profitable manner is a threat. Therefore, the solution to part of the problem is in having a disaster recovery plan in place in event of a disaster.

The data shows that the major aspects that would be required for an organisation to prepare for a disaster event are management support, carrying out a risk analysis and business impact analysis and having a disaster recovery plan in place. It is recommended that management be involved in all aspects of the disaster recovery planning as they set the standards of the organisation. Management would help develop and approve the

disaster recovery plan and policies pertaining to disaster recovery, ensure that all employees are aware of the disaster recovery plan, and the policies thereof as well as enforce the policies.

The data also suggests that carrying out a risk analysis and a business impact analysis would aid the business in formulating the disaster recovery plan. The risk analysis would aid in determining which threats are the most likely to happen within the environment an organisation is operating within. The impact analysis would enable the organisations evaluate the impact the threats would have on their business and thus put in place measures to ensure availability of information for business continuity.

The data also suggests that the organisations require a disaster recovery plan. This would ensure that, there are clearly laid out procedures to mitigate the effect of a disaster event and also, in event of a disaster that procedures exist to ensure that business continuity and that there is recovery and finally restoration of the business.

In all, the above recommendations for organisations both within the Nairobi Stock Exchange and others that are not listed, are indicated as capable of ensuring that they are prepared for disaster events to ensure that, there is business continuity and that there is mitigation measures in place.

CHAPTER 5: SUMMARY, CONCLUSIONS, LIMITATIONS AND SUGGESTIONS FOR FURTHER RESEARCH

5.1 Introduction

The objective of the study was to determine the aspects of disaster recovery, the importance that companies have assigned to these aspects and the challenges they face in effecting disaster recovery management programmes. The study was carried out among companies quoted on the Nairobi Stock Exchange. This chapter summarises the key findings, concludes the study, outlines some of its limitations and provides directions for further inquiry in disaster recovery research.

5.2 Summary

The results indicate that, most of the respondents had worked in their organisations for over seven years. This could be the reason they have realised that the information on which they rely on for business decisions and continuity should be protected by having response and recovery measures in place in event of a disaster.

The number of employees was used to determine the size of companies quoted on the Nairobi Stock Exchange. It was realised that, the companies within the agricultural sector have the most employees probably because of their labour intensive methods.

Most companies have adopted the use of information and communication technology within their organisations due to the need for faster processing of information, the need for the information to be available as soon as it is needed and to improve overall performance. The study found that, all the respondent companies have most of the their functions computerised and thus, the increased need to protect their information.

The IT/IS departments are in place in 33 of the 35 respondent organisations with 20 of these companies having the department as an entity on its own within the organisation. It is important to have the IT/IS department independent from other departments within the organisational hierarchy in order for it to have its own autonomy to carry out is functions

and to avoid the conflict of interest that may be expected when it is under another department.

Most organisations also have an IT/IS policy and budget within the organisations. An IT/IS policy would lay out the guidelines, policies and procedures, responsibilities, compliance and control issues that would provide guidelines in event of a disaster or during preparation for such an event.

The Finance and Investments sector had the most number of employees working on disaster recovery within their organisations. It is important to note that that these companies are mostly banks and financial institutions and due to the need for constant data availability, they have had to invest more in backup and recovery strategies as well as employees dealing with disaster and recovery issues to ensure that they mitigate disasters and are prepared in event of a disaster.

Most employees in all sectors are computer literate and it would be deduced that they are aware of the need to have their data available for business continuity purposes.

The results in the data indicate that it is integral to involve management in disaster recovery planning. Management should be aware of the environment in which they operate their business, the threats that their information is exposed to, the laws and regulations that affect their information protection requirements and thus, have a responsibility to reduce threats that face their businesses by approving and enforcing the disaster recovery plan. It is management that must help develop and approve the written disaster recovery plan, and ensure awareness and support of the plan from the employees.

The results in the data highlight the need to do a risk analysis which enables the identification of threats (the perpetrator of an attack), vulnerabilities (the method of entity of the attack) and thus, comparisons can be made against countermeasures (firewalls, access control systems and others) to determine the probability of a risk.

A business impact analysis would help identify the processes that are critical to the profitability and continued viability of the business, help with the quantification of financial and operational impact on outage over time and help determine recovery priorities, recovery time and recovery amount for each application that supports a critical business process. It would thus aid in justification for costs associated with mitigation and developing recovery strategies and so create support and the proper level of funding for a disaster recovery project.

The data results imply that, having a disaster recovery plan in place with clearly documented procedures and processes as important. The plan would aid in evaluating the critical business systems and data and the impact of unavailability of such systems. It would enable the determination what the potential disasters would be, their impact on the business. The plan would aid in identification of costs of various recovery alternatives and their advantages. It would aid in identification of the disaster recovery planning team with the necessary skill and expertise, as they shall have the responsibility of guiding the organisation in terms of mitigation of disasters and preparation for disaster events to ensure recovery and restoration. Therefore, the plan would also enable, creation of responsibilities for the team members. Constant testing and training would enable awareness and preparation in event of a disaster among the employees and management as well as enable updating the plan. The creations of a disaster recovery plan overcome the challenge of lack of protection of data and information in terms of appropriate storage locations for purposes of backups. Thus, organisations that have the plan should constantly update it and those that do not have one, should embark on creating one.

5.3 Conclusions

In the dynamic environment today, organisations have come to rely on IT infrastructures not just as an aid to business, but for some, as the core of their business. As such, safe, secure and reliable computing and telecommunications are essential to these organisations. As these organisations begin to understand the importance of information security, and the need to have their data available for business continuity, they are developing mitigation and disaster recovery programs. Having a disaster recovery plan

in place would enable the organisation evaluate its threats and vulnerabilities, evaluate existing measures and what else should be done to safeguard their date, establish a disaster recovery team to direct the preparation for disaster events, facilitate the ongoing maintenance in terms of training testing and updating the plan as well as auditing. The disaster recovery plan would ensure that, proper storage procedures are followed to safeguard the data the organisation requires.

Overall, the results of the date indicate that, companies quoted on the Nairobi Stock Exchange are aware of the need to have the disaster recovery programmes within their organisation. This is critical especially in the current dynamic environment where organisations cannot afford to have downtimes of more that 48 hours and the fact that it is becoming increasingly necessary for many organisations to have a long-term strategic view of their business in terms of continuity.

Management has the responsibility to ensure continuity of the business and thus, have the responsibility to ensure that policies guiding the disaster recovery within their organisations exist and that all employees understand the procedures and what is expected of them for the success of such programmes. A disaster recovery programme includes more than just technology and people. It involves policies, procedures, audits monitoring, and an investment of time and money. Therefore, it is imperative that, management supports the disaster recovery programmes because they are able to tie their business continuity with the long-term strategic plans of the organisation. Management are also able to provide the scope and authority required by the disaster recovery team to be able to effectively manage the disaster recovery programme.

5.4 Limitations of the Study

A lot of methodological care and time has been put into this study but however, results must be interpreted cautiously. Several limiting characteristics of this study offer opportunities to researchers in this area as follows:

a) The respondents were mainly managers and did not involve end users views yet if a disaster event occurs, they are the most affected;

b) Time was a constraining factor for this study. Due to the inadequate time, it wasn't possible to guide all the respondents through the questionnaires and therefore, some of the questions would have been answered hurriedly; and

c) There has not been much research done in disaster recovery to provide adequate literature for more advanced research in the Kenyan social, economic and legal context.

5.5 Suggestions for further research

a) The study focused on managers in charge of information technology within the organisations. The study should be extended to include end users to avoid self-assessment bias of the managers and also because a disaster event would affect all employees in an organisation;

b) The scope of the study could be broadened to look at privately owned large companies. Such a study would be used to perform a comparative analysis against companies quoted on the Nairobi Stock Exchange;

c) Management is responsible for the preparation for disaster events. Thus is management willing to invest time and money to ascertain preparedness in event of a disaster in terms of creating and implementing disaster recovery programmes? and

d) Can organisations use their disaster recovery plans when a disaster event occurs? Had it taken into account the current disaster and had it been updated?

REFERENCES

Bates, R. J. (1991). **"Disaster Recovery Planning"**, McGrawhill Inc, New York

Bird, E. (2003). **"Targeting Preparedness"**, Disaster Recovery Journal, Volume 16, Issue 4

Blythe, B.T. (2003). **"False Cover: Could Inadequate Crisis Preparation Open You to a Charge of Negligent Failure to Plan?"** Disaster Recovery Journal, Volume 16, Issue 3

Chandler, R. C. and Wallace, J. D. (2004). **"The Business Value of Data"**, Disaster Recovery Journal, Volume 17, Issue 3

Croy, M. (2004). **"The Business Value of Data"**, Disaster Recovery Journal, Volume 17, Issue 3

Desouza, K. C. (2004). **"Simulating Disaster Scenarios A Missing Link in Crisis Management"**, Disaster Recovery Journal, Volume 17, Issue 3

Drucker, P. (1974). **"Management: Tasks, Responsibilities and Practices"**, New York, Harper and Row

Hannabus, S. (1987). **"Information and Decision Making"**, Industrial Management and Data Systems

Heidelberg, E. (2003). **"Engineering Challenges in Disaster Recovery"**, ABME International

Jackson, J. A. and Dec, D. A. (2002). **"Business Interdependencies: A New Look at Planning for Disasters"**, Disaster Recovery Journal, Volume 16, Issue 1

Jenkins, B. D. (1988). "**Security Risk Analysis and Management**", Countermeasures Inc, New York

Kildow, B. A. (2004). **"The Importance of a Comprehensive Training Programme"** Disaster Recovery Journal, Volume 17, Issue 2

Koehler, N. (2002). **"Public Sector Planning: Getting Beyond June An Emergency Response Plan in the Public Sector"**, Disaster Recovery Journal, Volume 16, Issue 1

Mawanda, Z. (2004). **"Disaster Management Act ... Who Should Start"**, Disasters, Volume 8

Miano, B. (2003). **"Key Considerations for Proactive Planning - How to Mitigate the Effects of Disaster Prior to an Event"**, Disaster Recovery Journal, Volume 16, Issue 4

Mutunga, J. (2004). **"Fires in the Urban Set-up"**, Disasters, Volume 2

Mutunga, J. (2004). **"Preparedness Against Fire Disasters – Taking Pre-Disaster Precautionary Options"**, Disasters, Volume 4

Myers, J. (2003). **"Effective and Efficient Disaster Recovery Planning"**, Disaster Recovery Journal, Volume 16, Issue 4

Maiwald, E. and Sieglein, W. (1991). **"Security Planning & Disaster Recovery"**, Tata McGraw-Hill, West Patel Nagar, New Delhi

Sharp, J. (2003). **"UK Businesses Neglecting Disaster Planning Reports CMI Survey"**, Facilities Management Survey

Southgate D. (2002). **"Planning is Key to Disaster Recovery**", TechRepublic

APPENDICES

APPENDIX I: COMPANIES LISTED ON THE NAIROBI STOCK EXCHANGE

Agricultural

1. Brooke Bond Kenya Limited
2. Kakuzi
3. Rea Vipingo Plantations Limited
4. Sasini Tea & Coffee Limited

Alternative Investment Market Segment

5. A Baumann Kenya Limited
6. City Trust
7. Eaagads
8. Express Kenya Limited
9. Kapchorua Tea Company
10. Kenya Orchards Limited
11. Limuru Tea Company
12. Standard Newspapers Group
13. Williamson Tea Kenya Limited

Commercial and Services

14. Car & General (K) Limited
15. CMC Holdings
16. Hutchings Biemer Limited
17. Kenya Airways
18. Marshalls (EA) Limited
19. Nation Media Group
20. Tourism Promotion Services (Management) Limited
21. Uchumi Supermarkets

Financial and Investment

22. Barclays Bank of Kenya Limited
23. CFC Bank Limited
24. Diamond Trust Bank Kenya Limited
25. Housing Finance Company of Kenya
26. ICDC Investments Company
27. Jubilee Insurance Company
28. Kenya Commercial Bank Limited
29. National Bank of Kenya
30. National Insurance Credit Bank Limited
31. Pan Africa Insurance Holdings
32. Standard Chartered Bank (K) Limited

Industrial and Allied

33. Athi River Mining Limited
34. Bamburi Cement Limited
35. BOC Kenya Limited
36. British American Tobacco (K) Limited
37. Carbacid Investments
38. Crown Berger Kenya Limited
39. Dunlop Kenya Limited
40. East African Cables Limited
41. East African Portland Cement Company Limited
42. East African Breweries Limited
43. Firestone East Africa (1969) Limited
44. Kenya Oil Company Limited
45. Kenya Power & Lighting Company Limited
46. Mumias Sugar Company Limited
47. Total Kenya Limited
48. Unga Group Limited

APPENDIX II: LETTER OF INTRODUCTION

Dear Respondent

MBA RESEARCH PROJECT

This questionnaire is designed to gather information on the current status of information technology disaster recovery among companies quoted on the Nairobi Stock Exchange. This study is being carried out for a management project paper as a requirement in partial fulfilment of the degree of Master of Business Administration of the University of Nairobi.

All the information you disclose will be treated in strict confidence and will not be used for any purpose other than academic. I hereby undertake not to make direct reference to your name or your organisation in any presentation or report.

I would appreciate any additional information – in form of suggestions and comments, which you may deem necessary to enrich my research findings.

Thank you

Yours faithfully

AGNES NYAMBURA
MBA STUDENT

MR J LELEI
SUPERVISOR
FACULTY OF COMMERCE

APPENDIX III: QUESTIONNAIRE

Please answer the following questions by placing a mark (x) in the appropriate box or by giving the necessary details on the provided space.

SECTION A: DEMOGRAPHIC FACTORS

Respondent's Profile

1. Title or position of the respondent in the firm .....

2. Number of years in the organisation .....

3. How would you describe your main job role?
   Information Technology Manager []
   Disaster Recovery Director []
   Other (Specify) .....

Organisation's Profile

4. How long has your organisation been in operation in Kenya?
   From incorporation .....
   As a listed company of the Nairobi Stock Exchange .....

5. What is the ownership structure of the organisation?
   Foreign owned []
   Locally owned []
   Both locally and foreign owned []

6. In which of the following categories does your firm fall?
   Agricultural []
   Commercial and Services []

Finance and Investment []

Industrial and Allied []

Alternative Investments Market Segment []

7. a) How many people are employed in your organisation?

.....

b) How many of these employees are involved in disaster recovery?

.....

8. What is the level of information technology utilisation in the organisation

High []

Average []

Low []

9. What functions within your organisation are computerised?

Payroll []

Stock ordering []

Customer base management []

Supplier base management []

Payments management []

Invoicing []

Computer aided design []

Other, specify .....

.....

.....

10. a) Is there an information technology (IT) or information systems (IS) department within your organisation

Yes []

No []

b) If your answer to question 13 (a) above is yes, what is the position of the information technology department relative to other departments in the organisation hierarchy (eg, is it under finance or other department or is it independent)? .....

c) How many people are employed in your organisation in the IT or IS department?

.....

d) What is the turnover per annum on average for your organisation?

.....

e) Does your organisation have a budget for the IS or IT department?

Yes []

No []

d) Is there an IT or IS policy in your organisation? .....

.....

11. Please answer the following question by marking accordingly in the box that best describes how you would rate computer and information literacy within your organisation for the following category of staff.

	Poor	Average	Excellent
Executive director			
Top management			
Middle management			
Lower management			
Other staff			

SECTION B: ASPECTS OF DISASTER RECOVERY

12. The following are aspects of disaster recovery. For each aspect, please mark in the appropriate box the extent to which each is used in your organisation as regards your business needs and functions. Use the 5-point scale where:

    1. Not at all
    2. Very little extent
    3. Moderate extent
    4. Large extent
    5. Very large extent

		Not at all	Very little extent	Moderate extent	Large extent	Very large extent
1	Management is sensitised on the criticality of the information systems and applications required					
2	The importance of supporting disaster recovery plan for success is recognized by management					
3	Priorities for recovery in event of a disaster have been laid out					
4	The organisation's philosophy for disaster recovery is clearly articulated by management					
5	The organisation's finance and time availability are taken into consideration during disaster recovery planning					
6	Goals for recovery and restoration of business have been outlined.					
7	The disaster recovery team provides leadership on necessary actions in event of a disaster					

		Not at all	Very little extent	Moderate extent	Large extent	Very large extent
8	There are policies and procedures governing communication to all stakeholders and media					
9	There is a disaster recovery team in the organisation					
10	There is a disaster recovery department that deals with disaster recovery issues					
11	The disaster recovery team is composed of appropriate individuals in terms of leadership, skills and trustworthiness					
12	The disaster recovery team and includes members from all business units					
13	Members of the disaster recovery team have specific job descriptions					
14	The need for a budget for disaster recovery planning is recognised by management					
15	There are laid out alternatives and replacements in terms of resource and systems in event of a disaster.					
16	Key personnel within the organisation are involved in identifying business critical areas.					
17	Threats and vulnerabilities facing the organisation have been identified					
18	The organisation has analysed and categorised its risks					
19	Measures have been put in place to reduce identified risks					
20	The business processes have been analysed and prioritised in terms of criticality					

		Not at all	Very little extent	Moderate extent	Large extent	Very large extent
21	Procedures are laid out on determining if an event is a disaster or not and action to be taken					
22	The business has identified the impact to its operations if certain external groups failed to execute required functions					
23	There is legal counsel within the organisation to offer competent legal advise					
24	There are manual processes in place to support overall business objectives in event of a disaster					
25	There exists a disaster recovery plan					
26	The documents that helped publish the disaster recovery plan are available					
27	There exists procedures for communicating with employees during response and recovery after a disaster event					
28	There exists disaster recovery procedures that relate to direction, control and administration					
29	Departments have formal procedures stipulating what is to be done in the event of a disaster					
30	Inventory in terms of all assets of the organisation are held					
31	The disaster recovery plan documents the steps to be taken during a disaster					
32	There is constant testing of the disaster recovery plan in different scenarios					

		Not at all	Very little extent	Moderate extent	Large extent	Very large extent
33	Employees are involved in testing the disaster recovery plan					
34	There are clear roles and responsibilities for testing the disaster recovery plan					
35	There exists an awareness campaign to inform employees of ongoing disaster recovery planning efforts					
36	Employees are involved in training programmes					
37	The disaster recovery team members have a checklist of actions to help them understand their duties					
38	There is constant drilling and training of the disaster recovery team on the procedures					
39	There exist procedures on restoring facilities and normalizing operations after a disaster					
40	There are constant reviews and updating of the disaster recovery plan					
41	There exists an insurance policy for the assets that could be affected in case of a disaster					
42	The information technology department has processes in place to ease recovery of damaged computer systems					
43	There is constant evaluation of laws and regulations to ensure compliance					
44	Audits are often carried out as a risk management tool					

45. How often is testing of the disaster recovery plan done?

a) Whenever new policies and procedures are introduced

b) Monthly

c) Quarterly

d) Half yearly

e) Annually

f) Never

Other (specify) .....

46. How often is the disaster recovery plan updated?

a) Monthly

b) Quarterly

c) Half-yearly

d) Annually

e) Never

Other (specify) .....

47. Other aspect of disaster recovery (specify) .....

SECTION C: IMPORTANCE OF ASPECTS OF DISASTER RECOVERY

13. Rate the level of importance your organisation attaches to the following aspects of disaster recovery? Use a 5 point scale where:

1. Not important at all
2. Somewhat important
3. Important
4. Very important
5. Extremely important

		Not important at all	A little important	Moderately important	Largely important	Extremely important
1	Management support					
2	Identification of the criticality of the information system and applications					
3	Clearly laid out recovery and restoration priorities					
4	Proper communication procedures for stakeholders and media					
5	Existence of a disaster recovery team					
6	Autonomy and authority for the disaster recovery team					
7	A department dealing with disaster recovery issues					
8	Specific job descriptions for members of the disaster recovery team					
9	Alternatives and replacements for infrastructure and resources					
10	Procedures on handling external interdependent groups					
11(a)	Identification of risks, vulnerabilities and exposures					
b)	Measures for dealing with risks, vulnerabilities and exposures					
12	Identification of key disaster recovery procedures and processes					
13	Involvement of all business units in disaster recovery planning issues					
14	Technological expertise and experience of the disaster recovery team					

		Not important at all	A little important	Moderately important	Largely important	Extremely important
15	Proper budgeting and financing for disaster recovery planning					
16	Legal department to offer legal counsel					
17	Existence of a disaster recovery plan					
18	Training employees on disaster recovery (user awareness and education)					
19	Employees involved in testing the disaster recovery plan					
20	Constant review and updating the disaster recovery plan					
21	Alternative manual processes					
22	Insurance related policies or coverage in event of a disaster have been effected					
23	Insurance policy in event of disaster					
24	Procedures for communicating with employees in event of a disaster					
25	Inventory of organisations asset is available					
26	Constant drilling and training of the disaster recovery team members					
27	Evaluation of laws and regulations for compliance					
28	Audits for risk management					
29	Other (specify)					

SECTION D: CHALLENGES IN IMPLEMENTING DISASTER RECOVERY

14. Indicate by ticking the degree to which you agree with the following statements in respect of challenges encountered in your organisation during the implementation of disaster recovery programme

    1. Strongly agree
    2. Agree
    3. Neither agree nor disagree
    4. Disagree
    5. Strongly disagree

		Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
1	The scope and authority of disaster recovery issues is limited to the IT or IS departments only					
2	Management does not support disaster recovery issues					
3	There is no information on the criticality of the systems and applications					
4	There is no quantification of the cost of unavailability of systems					
5	There are insufficient funds to support the implementation of a disaster recovery programme					
6	There is a lack of awareness among employees on the existence of a disaster recovery plan					
7	There is a lack of internal commitment to disaster recovery					

		Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
8	There is no protection of data and information					
9	There is no proper design of the storage system for purposes of backup					
10	There lacks proper documentation of procedures and processes					
11	There lacks skills and expertise amongst the disaster recovery team					
12	Employees are not trained on what to do in event of a disaster					
13	There is no testing of the disaster recovery plan					
14	The organisation structure does not cater for a disaster recovery department					
15	The impact of a disaster on the survivability of the business has not been identified					
16	There is lack of proper coordination of the disaster recovery programme					
17	There is a lack of proper mechanisms to facilitate reviews of the disaster recovery plan					
18	Other (specify)					

THANK YOU FOR TAKING TIME TO FILL IN THIS QUESTIONNAIRE.