FACTORS AFFECTING AUTOMATED BUSINESS RECOVERY AT NATIONAL SOCIAL SECURITY FUND, UGANDA

BY

IMMY BYARUHANGA
07/MMS MGT/13/087
PGDCS(MUK), CCNP(UK), CISSP(USA), BSC Ed (MUK)

Supervisors
Mr. Onweng Tobias
Uganda Management Institute

Mr. Ochieng Denis
National Social Security Fund

A DISSERTATION SUBMITTED TO THE HIGHER DEGREES DEPARTMENT IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTERS DEGREE IN MANAGEMENT STUDIES (MANAGEMENT OPTION), OF UGANDA MANAGEMENT INSTITUTE.

SEPTEMBER 2010

DECLARATION

I **Immy Byaruhanga** , do declare that this research report is my own, unaided work, except as indicated in the acknowledgements, the texts and references and has not been presented by anyone else to any academic institution for any award.

Signed----------March 12, 2009

Mr. Immy Byaruhanga, Research Student

APPROVAL

The work contained in this study has been supervised by:

Signed----------

Mr. Ochieng Denis, Work- Based Supervisor

Signed----------

Mr. Onweng Tobias, UMI- Based Supervisor

DEDICATION

This dissertation is dedicated to Mylia Rubanzana my sister for the support and encouragement she offered to me before and during the study. I also appreciate the love and interest she reserves in the fields of service sustainability and business continuity.

ACKNOWLEDGEMENT

I would like to take this opportunity to express my sincere appreciation and gratitude to my supervisors, Mr. Onweng Tobias- UMI based supervisor and Mr. Ochieng Denis – work based supervisor, for their time and invaluable knowledge that has guided me through out my study to produce this dissertation.

Special thanks go to The Honourable Professor Tarsis Bazana Kabwegyere, Minister of Relief, Disaster Preparedness and Refugees for his insightful discussion on Disaster Preparedness in Uganda.

Indeed my sincere appreciation goes to the management and staff of National Social Security Fund (NSSF) who were candid in all their responses.

ACRONYMS

BCP	Business Continuity Plan
BOU	Bank of Uganda
DRP	Disaster Recovery Plans
FGD	Focus Group Discussion
Ha	Alternative Hypothesis
ICT	Information and Communication Technology
IMIS	Integrated Management Information System
IT	Information Technology
MDT	Minimum Down Time
NIST	National Institute of Science and Technology
NSSF	National Social Security Fund
RTO	Recovery Time Objective
SLA	Service Level Agreement
SPSS	Statistical Package for Social Scientist
SSDMS	Social Security Database Management System
UMI	Uganda Management Institute
UTL	Uganda Telecom Limited

Definition of Terms

Access Privileges: These are permissions set on information system users' accounts. User Bob may have permission to only read a file while Paul may have permission to read and write to the same file.

Activation: Activation is a start time when all or portion of the recovery plan is put in motion

Activation plans: These are well documented procedures that must be followed and actions that must be performed before, during and after a disaster has been detected and eventually communicated

Backup: Backup is the activity of copying files or databases so that they will be preserved in case of equipment failure or other catastrophe.

Cold Sites: A cold site is a similar type of disaster recovery service that provides office space, but the customer provides and installs all the equipment needed to continue operations.

Disaster Recovery Sites: A backup site is a location where an organization can easily relocate following a disaster, such as fire, flood, terrorist threat or other disruptive event.

A backup site can be another location operated by the organization, or contracted via a company that specializes in disaster recovery services. In some cases, an organisation will have an agreement with a second organisation to operate a joint backup site. This is an integral part of the

	disaster recovery plan and wider business continuity planning of an organization.
Disaster:	Disaster is an unanticipated loss of the ability to provide full service to both field units and the civilian population
Disaster Recovery Plan:	Outlines the procedures for collecting and conveying information immediately following a business interruption. The process involves the analysis of every aspect of the organization's management so that the company is positioned to survive the erosive effects of the winds of change, emergency or crisis.
Hot Sites:	A hot site is a commercial disaster recovery service that allows a business to continue computer and network operations in the event of a computer or equipment disaster.
Human Capital Development:	This involves the training, simulations, drills and general skills development of employees in a given corporation. **Risk:** The exposure to unwanted loss or the measure of likelihood and the consequence if a particular threat is realised.
Threat:	Anything with potential for adverse effect.
Vulnerability:	Susceptibility of a resource to a threat, for example no door to data centre.

Warm Sites: A warm site is compromise between hot and cold. Such sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. Warm sites will have backups on hand, but they may not be complete and may be between several days and a week old.

TABLE OF CONTENTS

DECLARATION II

APPROVAL III

DEDICATION IV

ACKNOWLEDGEMENT V

ACRONYMS VI

DEFINITION OF TERMS VII

TABLE OF CONTENTS X

ABSTRACT XIII

CHAPTER 1 1

1.0 INTRODUCTION 1
1.1 Background to the Study 6
1.2 Statement of the problem 7
1.3 Objectives of the study 8
1.4 Research questions 9
1.5 Statement of hypotheses 9
1.6 Significance of the study 10
1.7 Scope of the Study 10
1.8 Conceptual Framework 11
1.9 Chapter Outline 13

CHAPTER 2 14

LITERATURE REVIEW 14
2.0 Introduction 14
2.1 Effect of recovery facilities on business recovery 15
2.2 Effect of Activation Plans on automated business recovery 16
2.3 Effect of human capital on business recovery 17
2.4 Effect of Government and Service provider infrastructure on automated business recovery 18

CHAPTER 3 19

RESEARCH METHODOLOGY 19
3.0 Introduction 19
3.1 Research Design 19
3.2 Study Population 19
3.4 Sampling Technique 19
3.4 Sample Size and Selection 20
3.5 Data Collection Methods 21
3.7 Procedure of Data Collection 24
3.7 Data Analysis 25
3.8 Measurement of variables 26
3.9 Limitations of the Study 26

CHAPTER 4 28

PRESENTATION, ANALYSIS AND INTERPRETATION OF RESULTS 28
4.0 Introduction 28
4.1 Business and Disaster Recovery Facilities at NSSF 28
4.2 Activation Plans at NSSF 33
4.3 Human Capital and Automated Business recovery at NSSF 37
4.4 Government Policies and Service Provider Capacity and Automated Business Recovery .. 40
4.5 Vulnebility and Impact Assessment at NSSF 46

CHAPTER 5 50

SUMMARY, DISCUSSION, CONCLUSION & RECOMMENDATIONS 50

5.1 Introduction *50*
5.2 Summary..... *50*
5.3 Discussion *51*
5.4 Conclusion..... *56*
5.5 Recommendation..... *57*

List of Tables

Table 3.1: Distribution of Sample Size ……..13

Table 4.1.1: Does NSSF outsource recovery services from commercial hot, or cold sites ……29

Table 4.1.2: Does NSSF have data storage like such as back-up tapes, CDs,……...30

Table 4.1.3: does NSSF do Electronic vaulting for its of data ……31

Table 4.1.4: Does NSSF own a disaster recovery centre for its of data and applications……...31

Table 4.1.5: Are there Redundant or backup links between data centre and branch offices……...32

Table 4.1.6: Remote disk mirroring facilities at NSSF……33

Table 4.1.7: Does NSSF carryout regular disaster simulations to test readiness for automated recovery……33

Table 4.2.1: Does NSSF have disaster recovery plans available for execution……34

Table 4.2.2: Are there disaster recovery strategic plans at NSSF ……34

Table 4.2.3: Are the disaster recovery plans integrated in the corporate culture at NSSF……..35

Table 4.2.4: Has NSSF done a disaster vulnerabilities exercise and carried out a Business Impact Analysis…….36

Table 4.2.5: Activation Plans and Automated Business Recovery in percentages……....36

Table 4.2.6: Relationship between activation plans and automated business recovery……...37

Table 4.3.1: Is there Employee sensitization of organization's disaster recovery strategies……38

Table 4.3.2: Are there Staff to activate DRP/BCP for mission in critical systems……...39

Table 4.3.3: Human capital and automated business recovery at NSSF……39

Table 4.3.4: Relationship between human capital and automated business recovery……...39

Table 4.4.1: Is there a government policy on data and business recovery……40

Table 4.4.2: Does Government audit NSSF's business recovery plans……41

Table 4.4.3: Does Government aid corporate business entities to recover from disasters……42

Table 4.4.4: Is Business Continuity part of government's disaster preparedness program……43

Table 4.4.5: Do Services providers' have enough capacity to provide data communication services across the country……44

Table 4.4.6: Are there Data hosting and outsourced DRP programs available from service providers for client enterprises……45

Table 4.4.7: Are costs of establishing connectivity affordable to most enterprises……46

Table 4.4.8: Relationship between Government and Service Providers in positioning institutions for automatic….46

Table 4.5: How the occurrences of the disaster affect service delivery in an organization……47

List of Figures

Figure1.1: The Conceptual Framework…….....12

Figure4.2: Routine disaster simulation and recovery schemes at NSSF…… ..35

Figure4.3: Human Capital's ability to respond to Indicators of Disasters at NSSF……..41

Figure4.4: Provision of Guidelines by Government Through Relevant Ministries to Public and Commercial Business Entities for Implementing and Maintaining Business Recovery Programs……43

Figure4.5: NSSF has implemented data security systems ……47

ABSTRACT

The purpose of the study was to examine the factors affecting automated business recovery at National Social Security Fund (NSSF). More specifically, the study considered three critical factors that affected automated business recovery namely; the activation plans, human capital and modulator effect of government policies.

The study employed the descriptive research design and both the qualitative and quantitative approaches were used in the collection, analysis and presentation of the data.

It is evident from that study that NSSF has invested in human capital and equipped them with the requisite skills to manage disasters. NSSF has also provided for in service training to a select team in the area of business continuity. The study finds that a number of disaster recovery strategies have been acquired and are running at NSSF but they are not sufficient enough to trigger automated business recovery. The study recommends that a comprehensive enterprise wide business recovery program be acquired and should in detail cover all aspects of recovery facilities, human capital, activation plans because of their direct relation with automated business recovery.

Chapter 1

1.0 INTRODUCTION

This study examines factors affecting automated business recovery at National Social Security Fund (NSSF) which is a national organization responsible for the custody of the eligible citizens' social security. NSSF is a provident fund (pays out contributions in lump sum). It covers all employees in the private sector including Non Governmental Organizations, that are not covered by the Government's pension scheme. It is a scheme instituted for the protection of employees against the uncertainties of social and economic life. It vision is to be the region's leading Social Security provider, delivering a wide range of quality products and services and a real return to our members, while driving economic development and sustaining a competitive advantage in a free market. It is currently a custodian of a fund over USD 1.5Billion and a clientele of 350,000 members. Annually, NSSF collects over USD 120Million in contributions and pays out approximately USD 30Million in benefits. NSSF commits to providing a convenient and efficient system to employers, for the purpose of meeting their own and their employees' NSSF obligations and any means to ensure that it provides the best service is its fundamental objective. The study is salient because for an organization of its magnitude, work and sensitivity, information safety is paramount. In order to realise this vision, NSSF has invested in a robust information system that manages all major line of business functions for the enterprise.

In the study recovery facilities, activation plans and human capital were examined as factors affecting business recovery in case of a disaster or catastrophe occurring with

a view to establish if NSSF has coherent programs in place to ensure recovery and therefore business continuity

Determining what historical events constitute as a disaster is not a clear-cut matter. In nearly every case where disasters have been mentioned, partisans of various sides have fiercely disputed the interpretation and details of the event, often to the point of promoting wildly different versions of the facts. However with businesses and organizations where financial, jobs, systems, and material losses have been registered, effects cannot be ignored. Disasters are seen to have had a great historical dimension and businesses have closed while in some instances others are seen to have survived by having in place plans for loss mitigation.

Theoretically, the importance of business survival in an uncertain world was re-affirmed by Nemzow (1997), who stated that major business interruptions particularly those featuring dramatic disasters grab attention and focus it on one vector of threat at a time. According to him, it is important, however, to keep the broad perspective, in mind. Although business continuity planners naturally check their own company's vulnerability to the natural or man-made disaster making news at the moment, the economic trends of the past 18 months demonstrate that the greatest threat to most businesses is simply "less business." Factors to consider for business survival are complex, extending beyond data security and physical security. Being prepared for business interruption involves analysis of every aspect of the organization's management so that the company is positioned to survive the erosive effects of the winds of change. Business disruptions whether as result of natural disasters, technology failures or criminal acts can threaten the very survival of a company. Such disruptions cannot always be predicted or prevented, but sound planning can

dramatically reduce the damage they cause and effective preparation for disaster recovery and business continuity is a job for every company.

In the era of information systems and distributed computing, most businesses of which NSSF forms part no longer have the luxury of several days to fix a problem. In fact, most critical applications, like those used in e-commerce and customer service, usually require continuous availability or the recovery of data and critical applications in minutes and at worst, several hours incase of information system disaster.

Hiles (1992) defines an information system disaster as: "An event which causes the loss of the communication services or of a significant part of it, or of systems, communications or applications for a length of time which prevents the impacted organization from achieving its mission or which imperils the business". The impact may be felt in a number of different ways:

- Existing customers may transfer business elsewhere, and prospects may not be converted into new customers.
- New business is strangled; even loyal customers quickly become disaffected and hard-won market share drops.
- The organization's image and credibility may be damaged beyond recovery.
- Cash flow goes into reverse as creditors seek immediate payment and debtors defer settling bills knowing that credit control systems are not available to purse them.

According to the Gartner Group, two out of five companies that experience a catastrophe, or an extended system outage never resume operations; and of those that do, one-third go out of business within two years (Eklund, 2000).

These facts lead to the conclusion that every company must be prepared for recovering from possible disasters. The object of disaster recovery is not to eliminate risk, but to manage it. A disaster recovery plan should comprise several elements including immediate reaction procedures, restoration of the computing infrastructure, restoration of the applications, resumption of business processing under emergency arrangements, and restoration of the primary computing service.

The key challenge of business continuity preparation is not technology, but the internal marketing "business" aspects such as, justification for a business continuity project, executive buy-in, broad organizational support, and governance and politics. According to Burton (1998) perhaps the most important point to make about business continuity support technologies is that their effectiveness depends entirely on the organization's top-down commitment to the entire business continuity/disaster recovery project, including the updating and testing necessary for maintenance.

Further Davis (2003), in his study on developing business continuity in government planning found out that business infrastructure remains less protected than its stewards think it is, and such surprises usually lie in failure to consider the full scope of issues that continuity planning must encompass. According to him, two curable causes of disappointing continuity plan performance may be viewed as "spotty plans" (with gaps) and "plan rust" (from inadequate testing). Testing is expensive, and a company's commitment to it may depend on the perceived cost of disruption which can be less than feared through the use of selected testing tactics, such as broad-brush walkthroughs for logistics and "worst case" scenario exercises limited to the most likely events and the highest-cost risks.

Successful plans must be updated and tested regularly; a process which includes re-training employees in their roles, re-training that should include practice in thinking

nimbly and creatively in worst-case scenario examples. Such nimble thinking demands thorough knowledge of available resources and other elements of the continuity and recovery plan. Such plans share several characteristics: executive and board-level support; clear concise directions for action at every level; Integration with the corporate management culture, as an ongoing activity; Inclusion of risk management considerations; Prioritization of vulnerabilities; Coordination with suppliers and customers; and continual internal marketing to maintain participant awareness and motivation, with regular "what if" drills in creative solution implementation.

In Uganda, NSSF's business continuity and disaster recovery strategies rely more on storage on one set of servers which are situated in one location instead of also having a recovery site at any other regional office. They also rely on tape backups which are periodically scheduled. According to Park (2003), no back up failure is good and that the biggest mistake made in technology circles today is forgetting that technology exists to serve the business. This is because for many years, most IT managers are still relying on tape backups as the cornerstone of their disaster recovery and data protection infrastructure because a tape is reliable and portable, Baltazar (2003) and NSSF is no exception.

However, the biggest problem with tape backups is that data between backups is vulnerable, for example, if one's last backup was midnight and the storage system failed in the afternoon, any data created during the several hours between the last backup and the hardware failure event is lost. Baltazar (2003) noted that this problem with tape backup can be solved using data replication where data can be moved and synchronized between primary and backup sites in short amount of time, thereby

guaranteeing business continuity in case of disaster hence data and information security.

The core business functions of NSSF include registration of members, collection of members' contributions, managing Contributions, payment of workers' benefits, processing and disseminating relevant information to stakeholders for example issuing accountability reports and employee contribution statements.

In the case of Disaster Recovery program at NSSF, during the financial year 2006/2007 NSSF planned to implement a Disaster Recovery program and an amount of USD 503,024 was budgeted and approved for this purpose. It was later decided that instead of implementing a Disaster Recovery Plan ahead of major systems upgrade, a complete Business Continuity Program instead be planned.

According to Nemzow (1997), the best planning looks to diversification as a strategy for protecting an organization even with a direct disaster hit. Diversification does not mean creating backups and hot sites, but creating an infrastructure for control and coordination. This would enable all assets allocated to disaster recovery to be used all of the time and to be reallocated in the event of a disaster.

1.1 Background to the Study

NSSF has nine departments, which are Information Systems, Operations, Finance, Audit, Human Resource, Marketing and Communication, Investment, Administration, Legal and Risk Management. NSSF has employs close to 800 staff 650 of which are permanent and is headed by a management team comprised of the Managing Director, Deputy Managing Director, Corporation Secretary and Ten Heads of Departments. The Team works together in matters of management, administration and organization of NSSF. The organization has a Board of Directors who is responsible for making policies that govern it, and which have to be implemented most efficiently and

effectively for better service delivery. Currently, the organization's direct supervision is by Bank of Uganda under Ministry of Finance, Planning and Economic Development.

From 1994 to 2004, NSSF had an automated Database system called Social Security Database Management System (SSDMS) that was developed in FoxPro. The Database was installed on computers and running as a stand alone system at upcountry stations. At the headquarter station in Kampala, the Database was installed on a shared server. Hosts' access to the server was limited to within a Local Area Network and within a limited radius of a Metropolitan Area Network. Currently, SSDMS is an old Information Technology (IT) system whose key functions are phased out. In 2008 NSSF commissioned a new IT system, Integrated Management Information System (IMIS). The old system was standalone, data was distributed and it involved manual update to bring the data up-to-date. Even then, by the time an ample cycle is done, other changes would be due and in brief the database was never up-to-date. However with the IMIS, data stored in the database is online and the changes are done in real time. As the NSSF continues to upgrade its information systems to match with data and information requirements of its different stakeholders, so is the need to use modern tools and tactics to manage the process of business continuity and disaster recovery incase of catastrophe. This can only be achieved only if there is integration of business continuity planning in the overall corporate risk management framework at NSSF.

1.2 Statement of the problem

The provision of disaster recovery procedures is not a widely implemented concept in Uganda. Since 1994, NSSF has implemented various IT systems with enhancements to cater for data and information availability and security and all NSSF core functions

rely on data and information that are stored in these systems. The Central Bank in December 2004 made an examination of the IT systems at NSSF and pointed out lack of an operational business continuity strategy. Further, an audit carried out by PKF consulting Ltd for Auditor General in November 2005, to review the same IT system at NSSF, pointed out that the absence of Disaster Recovery Program (DRP) may lead to the loss of the entire IT investment and cripple NSSF operations.

Current operations at NSSF use over 35,000 sheets of paper every month in contribution schedules, benefit claims, payment advises and cheques, registration drafts and certificates and clearly this is more of a paper based institution that is not well managed and it would be difficult to manually fall back onto within the next 2 years incase of disaster. In spite of the efforts made to have a Disaster Recovery Program at the NSSF, it has continued to suffer indicators of what may culminate into a disaster. This could be attributed to the absence or inappropriate provisions for a DRP framework that may be tailored to meet BCP requirements. There is no research on why the indicators of a disaster still exist despite efforts to implement a DRP at NSSF. It is on this basis that there was a great need to carry out a study on factors affecting automated business recovery at NSSF.

1.3 Objectives of the study

1.3.1 General Objective

The objective of the study was to examine the factors affecting automated business recovery at National Social Security Fund.

1.3.2 Specific Objectives

i. To examine how recovery facilities affect automated business recovery at National Social Security Fund.

ii. To examine how activation plans affect automated business recovery at National Social Security Fund.

iii. To examine how human capital affects automated business recovery at National Social Security Fund.

iv. To assess the modulator effect of government policies and service provider capacity on the relationship between factors and automated business recovery.

1.4 Research questions

i. Why hasn't NSSF employed disaster recovery facilities to safeguard its data and information security?

ii. Why are there no documented, accessible and soundly communicated activation plans on disaster and its related disruptions at NSSF? What competences does NSSF have to deal with the different forms of disaster?

iii. What government policies guide information technology security and who is responsible for their implementation?

iv. What service providers are available to NSSF to ensure that it has the appropriate automatic business recovery system available to NSSF?

1.5 Statement of hypotheses

Ha_1: Automated Business Recovery can only be effective if there are disaster recovery facilities available at NSSF.

Ha_2: Automated Business Recovery can only be effective if there are activation plans in place at NSSF

Ha_3: Automated Business Recovery can only be effective if there are manpower capacity and IT disaster recovery plan.

Ha_4: Automated Business Recovery can only be effective if there are government laws and service provider infrastructure.

1.6 Significance of the study

From the above sections, it is clear that disaster recovery plan and business continuity is one of the most important requirements of an organization, and is critical to business. While the research was predominantly a requirement for a Masters Degree in Management Studies of the Uganda Management Institute (UMI), the results of the study would be invaluable to policy makers in charge of data management in big corporations.

Business recovery in any institution is of paramount importance and studies elsewhere have demonstrated that it is a prerequisite for effective management of institutions. Such a study has not been done at NSSF and therefore it is timely. It is envisaged that, the study will contribute to the thorough understanding of the fact that delay in business restoration may have exponential harmful effects and hence the need to analyze these challenges and suggest ways in which they could possibly be mitigated. This would in turn reposition NSSF to be more resilient though adoption of better management strategies especially in the light of competition that it faces ahead of the government policy of liberalizing the pension sector. In addition, the study will contribute to the body of knowledge on business continuity planning in Uganda and beyond.

1.7 Scope of the Study

1.7.1 Content scope

The study was restricted to evaluation of the factors affecting automated business recovery. More specifically, the study concentrated on factors such as disaster

recovery facilities, activation, human capital effects, government policies and service provider infrastructure.

1.7.2 Geographical scope

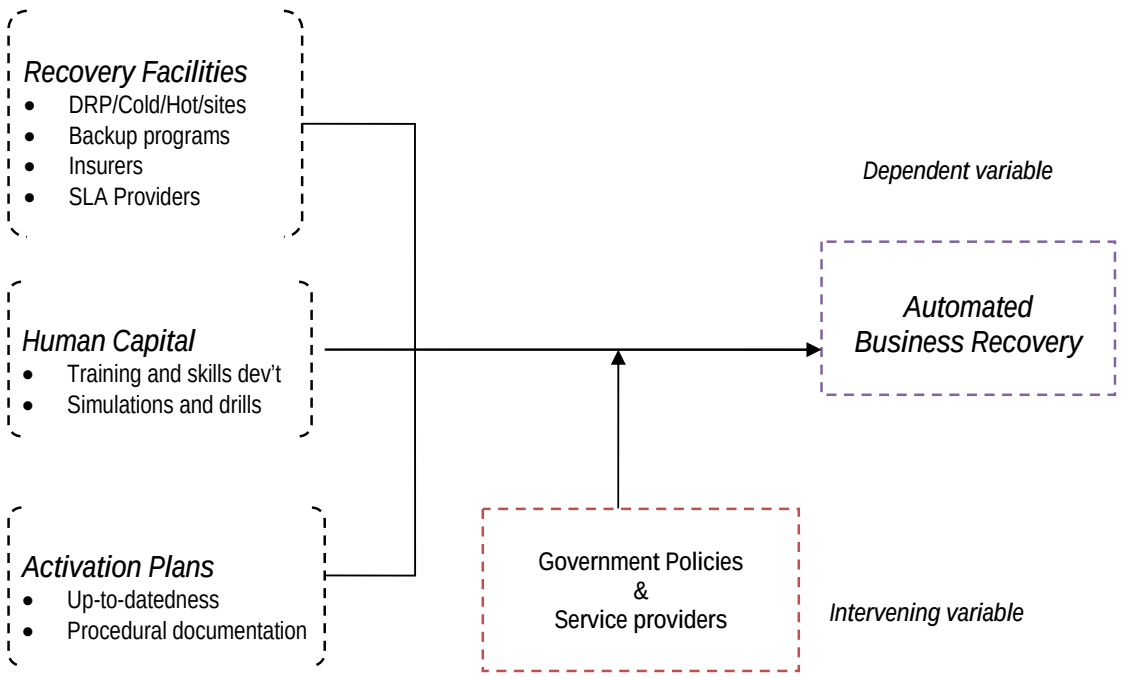
The study was carried out in National Social Security Fund. The Fund is located in Kampala City Centre along Pilkington Road, Workers House. This is because Workers' House accommodates the headquarters of the organisation and the data center where all data processing is done.

1.7.3 Time scope

The research reviewed and considered all works done and documentation available at NSSF from 2004 to 2009. This is because the work and information outside this scope not provide good relevance to subject matter.

1.8 Conceptual Framework

Figure 1: The Conceptual Framework



An organization that operates under a computerized business environment must put in place a disaster recovery program and business continuity strategy incase of a disaster. This strategy is summarized in form of a model comprising of a number of independent factors and dependent factors and moderating factors. In this model, recovery facilities, human capital and activation plans were the independent variables. Service providers and Government policies were a moderating/intervening variables and automated business recovery was the dependent variable.

The above conceptual framework suggests that, under stable and consistent government policies and the availability of service from service providers, Automated Business Recovery is influenced by the availability of *Recovery Facilities(such as* DRP/Cold/Hot/sites, Backup programs, Insurers, and SLA Providers among others); available stock of human capital (that involves the training and skills development of employees and Simulations and drills); and availability of *Activation Plans (such as* Up-to-datedness, and Procedural documentation*)*

From the model, the availability of recovery facilities, human capital and activation plans create a favorable Environment for Disaster Recovery Program and Business Continuity plan which in-turn leads influences positively automated business recovery and vice-versa.

The model suggests that, the availability of recovery facilities such as DRP, cold site, hot sites and backup programs in an organization, results into greater chances of recovering and restoring business normality incase of disaster struck and vice versa. More so, from the model an organization needs to invest in human capital that

included training and skills development of its employees and also subjecting them to regular simulations and drills in combating disasters.

Lastly, the availability of skilled human capital in an organization, implies the greater the chances of restoring business to normality incase disaster struck and vice versa.

1.9 Chapter Outline

This study is organized in five chapters. The first chapter has provided a background to the study, the statement of the problem, research questions and hypotheses, significance of the study, scope and ends with the conceptual framework. chapter two, the literature review focuses on the works that have been done on the subject matter within NSSF and elsewhere. This is followed by chapter three detailing the methodology and the challenges experienced during research. In the fourth chapter, the findings are presented analysed and interpreted. In the last chapter (Chapter 5), the study is summarised by discussing the research results and conclusions are drawn. The study also highlights practical recommendations to National Social Security Fund on how it can reposition itself to be more resilient by implementing reliable automated business recovery systems.

Chapter 2

LITERATURE REVIEW

2.0 Introduction

In this chapter the related literature about factors affecting automated business recovery in organizations is reviewed. Very limited studies have been undertaken in Uganda on this subject. Some companies however, with multi-national affiliation like DFCU Bank, Shell Uganda, Stanbic Bank have done work on identifying the most likely threats to their business, and have identified remediation activities that can be implemented, together with a Business Continuity Plan that gives clear instructions for recovering Critical Business Functions for most types of incident. Much of the existing literature on this subject was as a result of studies carried out in developed economies such as United States, Britain and Canada. In these countries there is a line of authority is clear right from the top leadership (President or Prime Minister) providing clear guidelines, to institutions and local authorities on how mitigate, respond and recover for disaster related incidences. It is incumbent of these entities to have a well formulated business continuity strategy that is achievable, regularly tested and auditable. In Uganda, the department of disaster preparedness and relief is relatively young having been established in 2001 and still at the stage of policy framework development. The ministry however, is concentrating on activities relating to floods, livestock restocking, resettling war victims and little or no attention is being given to Information and Communication Technology (ICT) related disasters and yet ICT is the life blood of well function business system.

Much of the literature reviewed in this chapter was therefore based on research undertaken in foreign countries. This nonetheless, did not undermine the findings of the study because the concepts remained basically the same. Literature review covered variables such as recovery facilities, availability of activation plans, organizational human capital and the modulator effect of government policies and service provider capacity on the relationship between factors and automated business recovery.

2.1 Effect of recovery facilities on business recovery

Recovery Facilities comprise of aids, tools, or infrastructure used in implementing a recovery program by a restoration of business functions like an information system. Many companies use separate buildings and facilities to house duplicates of **mission critical systems** that can be activated in a disaster. (http://www.idsemergencymanagement.com.) In cases where systems are replicated (hot sites), whenever there are changes on the primary site, the same change are replicated on the secondary site. This means that at any one time there are two sets of same data owned by the organisation which implies that if one site fails then the other site will continue to deliver service. These systems are installed in such a way that users of the system will experience no interruption during system change over. Regular disaster simulations are done quarterly or biannually and an assessment of recovery time objective or acceptable downtime is noted to determine its reliability. Cost and geographical proximity between sites are major factors to consider when planning to acquire a hot site however, hot sites are deemed the most reliable and accurate business recovery facilities. In Uganda, companies in the financial bracket as NSSF that are running hot sites include MTN Uganda , Standard Chartered Bank,

Bank of Uganda, Ministry of Finance, Shell Uganda Barclays Bank, Stanbic Bank etc. Some of these institutions have their recovery facilities as far as Nairobi and Harare. There are other recovery facilities where instead of building an own DRP, it can rent space on the system from where it can run business recovery services after related incidents occur at the production site.

DeSimone and Morris (2003) argue that, Backup strategies are a vital component of disaster recovery planning as they can greatly reduce the time for recovery. Completely mirroring data and using instantaneous backups, for example, allows for quick recovery to a backup system within minutes. According to Robb (2004), Organizations also need to test restorability of backups to ensure they can actually access data on their backup media, meet their disaster recovery responsiveness and recovery time objectives, and avoid recovery failures. Often overlooked but critical is the backup and recovery of end-user systems which are statistically more likely to cause certain types of disasters as they are not as effectively protected against fires and other disaster potentials as data centers or communications equipment rooms (Toigo, 2003).

2.2 Effect of Activation Plans on automated business recovery

Activation plans are well documents procedures that must be followed and actions that must be performed before, during and after a disaster has been detected and eventually communicated. It is not limited to the actions and procedures must include the persons responsible and how these actions will be performed.

Empirical evidence attests to the central role of a tested disaster recovery plan in disaster preparedness. Unlike companies without a disaster recovery plan for reacting to and recovering from a catastrophe, companies that experienced potentially

devastating disasters and that implemented tested contingency plans survived such events and continued to operate in the marketplace [Toigo, 2003].

A formal disaster or business continuity plan documents various aspects of disaster preparations. Clarke [2004] warns of symbolic plans, those unrealistic disaster contingency plans that are not based on actual expertise or experience, that over promise, that are published in fantasy documents that describe these hollow plans, and that create a dangerous false sense of security. Planning tends to be more effective when ideas are actually put to the test using simulation exercises of mock disasters (Flood, 2005 and Heller, 2004)to identify whether the plan actually works [Calderon and Dishovska, 2005].

Companies with untested or poorly tested plan find that they are not as protected as they expected [Robb, 2005]. However, many barriers to testing DR plans exist including resource constraints in terms of budget and people's time, and disruption to employees, customers, and sales and revenue stream [Veritas, 2004].

A challenging aspect of planning is the maintenance of the plan over time. The IT disaster recovery plan is a living document that needs to be updated as business processes and other aspects of the business change [Toigo, 2003], and as organizational learning from tests and deployment of plans in response to actual crisis indicate needed modifications. Redundant systems at a separate facility are one of the most reliable and expensive recovery strategies that lead to minimal loss of routine business operations, providing companies with the confidence to recover from almost any disaster [Toigo, 2003].

2.3 Effect of human capital on business recovery

Strong support from senior management is critical for virtually anything, including disaster recovery and business continuity [Calderon and Dishovska, 2005]. In the

absence of top management commitment to disaster and business continuity planning, the effectiveness of such plans may be questionable [Pearson and Clair, 1998]. Also, similar to quality initiatives, the way the entire organization perceives and deals with crisis, disaster, or business continuity planning and management is likely to greatly influence the adoption of success of IT disaster recovery [Smits and Ezzat, 2003]. Specifically, embeddedness has been used to describe that the business continuity process is not only evidenced among the top management team but manifests itself throughout the organization. Where disaster recovery and business continuity assume a more strategic role, organizations need to provide a management infrastructure for disaster recovery planning that helps with creating a behavioral readiness for disaster via provision of disaster/business continuity teams, regular drills, formal coordinators, and programs that create awareness and understanding of how crises and interruptions can threaten the organization's operations and survival (Herbane, Elliott, and Swartz, 2004, Smits and Ezzat, 2003).

2.4 Effect of Government and Service provider infrastructure on automated business recovery

Organizations may not bother in investing in disaster recovery and business continuity strategy because of several factors. These may include lack of compliance laws and enforcement as is the case of developed countries like the United States or the United Kingdom where it is a legal requirement. It may also be possible that lack of improved and well distributed infrastructure from service providers may be a limiting factor for companies to establish facilities for disaster recovery and business continuity. Where facilities are available, the question of affordability may not be ignore especially in Uganda where government may not be able to afford extending subsidies or where the economy may not support such service.

Chapter 3

RESEARCH METHODOLOGY

3.0 Introduction

This section presents the research design, study population, data collection methods, procedure of data collection, data analysis, and measurement of variables, it also discusses major issues that could contribute to the limitations of the study and the researcher overcome them.

3.1 Research Design

The study employed a descriptive research design because of its strength in quantitative data management. Both qualitative and quantitative approaches were used in data collection and analysis.

3.2 Study Population

Owing to the large number of employees at NSSF (approximately 800) a target (smaller) population was selected using stratified sampling method and it covered the stakeholders in IT network management, database administration, IT security, operations management, administration and risk management The area was chosen because the researcher believed that required data for the study would be easily accessed.

3.4 Sampling Technique

Purposive sampling was used in selecting respondents for this study. The stakeholders that normally get involved in IT disaster management and Business continuity, database administration, IT security, organizational IT network management and risk

management were heterogeneous in nature, and as such no single one could be taken to be representative of the target population.

Consequently, in sampling the respondents, stratified sampling was used in such a way that the respondents selected from each group or stratum produced a homogeneous representation of the accessible population from that stratum. According to Kothari (2004, p.63), strata are purposively formed and are usually based on the past experience and personal judgment of the researcher. The following criterion was used in selecting the strata:

1. Knowledge of IT security
2. Knowledge of IT networking
3. Knowledge of database administration
4. Knowledge of risk management
5. General knowledge in administration

Mugenda and Mugenda (1999, p.48) have argued that for greater accuracy in the findings, the number in each stratum should be based on the relative variability of the characteristic under study rather than proportionate to the relative size of each stratum in the population. This implies that the sampling fractions differed from stratum to stratum but the strata in the population had to be represented in the sample in the same proportion that they exist in the population (Amin, 2005, p.247).

3.4 Sample Size and Selection

The sample size of the study was 80 respondents. The sample size was obtained using the following formula, n= $\mathbf{Z^2PQ/e^{2,}}$ **(**Mugenda and Mugenda**).** The formula was used to compute the above sample size, where n is the required sample size, Z^2 is the abscissa of the normal curve that represents the level of confidence, e is the desired level of precision, p is the estimated proportion of an attribute that is present in the

population, and q is 1-p. In this study, the error margin was 5% resulting into 95% confidence interval, the level of precision was 10% and it was assumed that at least 70% of the population was in possession of the information about the study resulting into a sample size of the study 80 respondents.

This number of respondents spread uniformly across various departments as summarized in table 3.1 below.

Table 3.1: Distribution of Sample Size

Strata	Department name	Population	Sample size
1	Information Technology	144	28
2	Operations Department	384	18
3	Marketing/Public Relations	112	14
4	Administration	150	16
5	Risk Management	10	4
	Total	**800**	**80**

$z = 1.652$, $p = 0.7$, $q = 0.3$ and $e = 0.1$

therefore, $n = 1.652^2$ **x 0.7 x 0.3/0.1**^{2}

$n = 80$

3.5 Data Collection Methods

A mixture of data collection methods were used because of categories of the resource persons that would provide vital data for the study. Face-to face interviews were used individuals that would not find time to fill the questionnaire like The Minister of Disaster Preparedness and Relief, the Managing Director of NSSF and some Heads of Departments, the officials from Ministry of Information and Communication Technology. The Questionnaire was used respondents from National Social Security Fund as selected in section 3.4 of this chapter. The researcher also extracted data from

library, newspapers, Business journals, research reports, and internet and concentrated mostly on IT disaster management and Business continuity, database administration, IT security, organizational IT network management and risk management. Data obtained from these sources, was compared with the first hand information from primary sources so as to arrive at a conclusion.

3.5.1 Data Collection Instruments

Both qualitative and quantitative data was collected and used according to the following data collection tree.

3.5.1.1 Self-administered Questionnaires

The researcher used structured questionnaires to gather data from the staff/management of NSSF in relevant fields that would provide useful information

A structured questionnaire contained a list of possible alternatives from which respondents select the answer that best suits the situation (Mugenda & Mugenda, 1999). An unstructured questionnaire provides space for the respondents to freely express themselves. To encourage honest answers, close ended and open ended questions about the factors affecting automated business recovery were given to employees of National Social Security Fund to collect qualitative and quantitative data. Questionnaires were used because they are simple to administer and can be filled in at the respondents' convenient time. The questionnaires were designed in such a way that reflected the objectives of the study.

3.5.1.2 In-depth Interviews

The researcher also used interview guide to gather necessary data for the study. The researcher asked the top management of National Social Security Fund, officials of

Ministry of ICT and Disaster Preparedness and Relief. The questions asked were guided the strategic responsibilities held and in line with the objectives of the study so as to get first hand information. This instrument was used because it is quickest technique of collecting qualitative data and questions can be repeated clearly for the respondents so that they comprehend better. The researcher put side by side the interview guide responses with the answers given in the questionnaire so as to gather more knowledge and to gain insight about the problem under the study.

3.5.1.3 Documentary analysis

Important documents containing information related to the factors affecting automated business recovery were studied and screened according to content. The documents included: management controls and procedures, a list of disaster recovery facilities, guidelines on protection against natural/ accidental disasters among other. The documents gave more details about IT disaster management and business continuity practices at NSSF.

3.5.2 Pre-testing

For the purpose of data quality control, the researcher ensured that the study should collect reliable data and had to validate it by piloting the data collection instrument in a reputable organization. Additionally, the pre-testing exercised gave the researcher some insights of how the interview should be conducted, what should be the sequence of the question, how to entice the respondents to answer the questions and appropriate length of each interview.

3.5.2.1 Validity

Validity is the strength of conclusions, inferences or propositions. More formally, Cook and Campbell (1979) define it as the "best available approximation to the truth or falsity of a given inference, proposition or conclusion." To ensure that the study comes up with convincing conclusions, the research instruments were administered in Finance Trust (U) Limited before administering it to NSSF. The purpose of the pre-testing was to form appropriate questionnaire that the selected respondents would understand and also to allow the researcher to familiarize the terminologies used by the respondents in the IT disaster management and Business continuity, database administration, IT security, organizational IT network management and risk management.

3.5.2.1 Reliability

Reliability is the consistency of a measurement, or the degree to which an instrument measures the same way each time it is used under the same condition with the same subjects. In short, it is the repeatability of your measurement. While the pilot study was done at Finance Trust (U) ltd., another selected group at NSSF was given the same instrument and the results collected were compared to determine consistency. This pre-testing exercise enabled the researcher to identify question ambiguity and response categories, interview instructions and questionnaire length and also provided the insight into the level of understanding of both the respondents and the researcher.

3.7 Procedure of Data Collection

Owing to the sensitivity of IT disaster management and Business continuity strategies in organizations, a covering letter accompanied each questionnaire explaining the

purpose, importance and significance of the study to remove any suspicion or bias from the respondent. Some of the questionnaires were distributed personally by the researcher, while others were distributed through established structures within the sub-groups such as through heads of departments. The filled questionnaires were collected after fifteen (15) working days. In the process of collecting the data, the researcher asked the respondents in the IT disaster management and Business continuity, database administration, IT security, organizational IT network management and risk management various questions as guided by the questionnaire, relating to the factors affecting automated business recovery at National Social Security Fund using the interviews. Interviews were personally conducted by the researcher in the respondents' offices. The data collected from the interviews was essential in data collaboration and delivery of meaningful conclusions and recommendations.

3.7 Data Analysis

Qualitative and quantitative data collected was analyzed, arranged, tabulated and interpreted. **Quantitative data** was analyzed using appropriate computer packages (such as Statistical Package for Social Scientists or SPSS) which yielded the desired statistical output, measures of dispersion and measures of relationships (correlation coefficients). Results are presented in form of frequency tables and charts which are interpreted accordingly. Analysis of **qualitative data** was through descriptions of events and occurrences as gathered from the interviewees. Judgment was made on the basis of highest percentages or otherwise depending on the facts on the ground.

3.8 Measurement of variables

The coding system was used whereby numbers were assigned to characteristics or events in order to operationally define the variables. Two categories of measurement were used namely: the *nominal measurement* and *ordinal measurement*. The *nominal scale* of measurement applied to cases which had some common set of characteristics such as sex, level of decision making in the organization, level of experience among others. In nominal measurement, numbers were assigned only for purposes of identification but not for comparison of the variables being measured. *Ordinal measurement* was used not only to categorise the elements being measured but also to rank them into some order. Therefore the numbers in ordinal scale represented relative position or order among the variables. The variables were measured using constructed questionnaire scales, specifically the five rating likert scale. The study variables were measured using the constructs indicated under them where respondents were asked to give a rated opinion. The higher score indicated higher relationship. In addition the spearman's rank of correlation was used to determine the relationship between factors affecting automated business recovery and the ability of Information Technology systems to recover and restore services in case of interruptions or disruptions at NSSF.

$$R^1 = 1 - \frac{6 \Sigma d^2}{n(n^2 - 1)}$$

Where:-

n = Number of respondents

Ry = Ranks of respondents who said yes

Rn = Ranks of respondents who said no

d = Difference or deviation between Ry and Rn.

3.9 Limitations of the Study

While on the research, the researcher encountered various hindrance and these were;

1. The behaviors of some employees were unpredictable. Some staff members concealed information by not filling in the questionnaires and others did not associate well with the researcher by not taking the study as a serious issue which in turn hindered the collection of the required data for the study. Therefore, to overcome this, the researcher assured the respondents that the information given was to be treated with maximum confidentiality and was for academic purposes only. Also the respondents were not under obligation to disclose their identities.
2. Financial encumbrances: Lack of funds to print research proposal, questionnaires, and report and to meet transport costs delayed the research study to be presented to the board of examiners. To overcome this problem therefore, the researcher solicited funds from grants to complement personal savings to finance the research study so as to finish the study within the stated time frame.

Chapter 4

PRESENTATION, ANALYSIS AND INTERPRETATION OF RESULTS

4.0 Introduction

This chapter covers the presentation, analysis, and interpretation of findings of the study. The objective of the study was to examine the factors affecting automated business recovery at National Social Security Fund. In a bid to examine these factors, research instruments were distributed to respondents within National Social Security Fund and other institutions in line with the specific objectives of the study. The responses obtained were tabulated presented and interpreted, in tabular form and charts and analyzed.

4.1 Business and Disaster Recovery Facilities at NSSF

In examining how recovery facilities affect automated business recovery at NSSF, the researcher asked the respondents to indicate whether NSSF has outsourced recovery services In the table overleaf, responses to whether NSSF had outsourced recovery services from commercial hot sites or cold sites are presented.

Table 4.1.1: Does NSSF outsource recovery services from commercial hot, or cold sites

Responses	Frequency	Percentage
Yes	19	24%
No	61	76%

As shown in the table 4.1.1 above, 76% of the respondents reject the view that NSSF has outsourced recovery services from commercial hot sites, or cold sites. s 24% of the respondents accept it. This implies that NSSF is reluctant to institute and

implement a more comprehensive and a rigorous recovery facility to keep the Fund running during a period of displacement or interruption of normal operations. It should therefore eminent that NSSF is operating at risk yet it handles variety of functions such as registration of members, collection of members' contributions, investment of the collected contributions, and eventual payment of benefits to eligible members, processing and disseminating relevant information to stakeholders including issuing accountability reports and employee contribution statements. These are key transparency statement NSSF pledges to deliver in its vision. Some of this information is stored in hardcopy form and it makes it very susceptible to disasters like fires.

Respondents were further asked to indicate whether NSSF has data storage backup facilities such as tapes disks, CDS with up-to date information as back-up facilities. The results gathered are shown in the table below

Table 4.1.2: Does NSSF have data storage like such as back-up tapes, CDs, etc

Responses	Frequency	Percentage
Yes	70	88
No	10	12

From the table above, 88% indicated that NSSF has data storage such as tapes disks, CDS with up-to date information as back-up facilities. Only 12% of the respondents did not agree that NSSF has data storage such as tapes disks, CDS with up-to date information as back-up facilities. This is because a tape is most common facility for backup and disaster recovery almost available in most organizations. This is because its cheap, portable and fairly reliable. Baltazar (2003) argues that IT managers are still

relying on tape backups as the cornerstone of their disaster recovery and data protection infrastructure because a tape is reliable and portable.

In ascertaining whether NSSF does electronic vaulting where data is sent directly from the subscriber site to the hot site. The findings solicited therein were tabulated as follows

Table 4.1.3: does NSSF do Electronic vaulting for its of data

Responses	**Frequency**	**Percentage**
Yes	22	17
No	58	73

The results suggest that (73%) of the respondents reject the view that NSSF does electronic vaulting. Electronic vaulting is where data is sent directly from a production site to a commercial hot site for purposes of safe storage and disaster recovery. Only 17% of the respondents indicated that NSSF does electronic vaulting. This finding confirms that NSSF rely generally on CD, memory sticks/flash diskettes and tape disks as the major recovery facilities.

The study also tried to establish the fact that at NSSF owns a disaster recovery centre for Backup and off-site storage of mission critical data. The findings gathered are presented in the figure below

Table 4.1.4: Does NSSF own a disaster recovery centre for its of data and applications

Responses	**Frequency**	**Percentage**
Yes	30	37
No	50	63

Table 4.1.3 above summarizes backup and off-site storage facilities at NSSF. It is indicated that the majority (63%) of the respondents reject that at NSSF there is a disaster recovery facility owned by the Fund for Backup and off-site storage of data and applications. It was only 37% of the respondents of the respondents that accepted it. This confirms that the Fund continues to operate at a high risk considering the amount of data it holds and the value there of.

In finding out whether at NSSF there are redundant links or backup links to branch offices. The responses obtained there from are herein presented as follows

Table 4.1.5: Are there Redundant or backup links between data centre and branch offices

Responses	**Frequency**	**Percentage**
Yes	51	64
No	29	36

Table 4.1.5 above summarizes responses about redundant links or backup links to branch offices. It is indicated that the majority (64%) of the respondents accepted that at NSSF there are redundant links or backup links to branch offices while 36% of the respondents disagreed.

In finding out whether NSSF has remote disk mirroring facilities for the data centre and branch offices where data is replicated in real time so as to continuously update information to disaster recovery servers. The findings gathered are summarized in table 4.1.5 below.

Table 4.1.6: Remote disk mirroring facilities at NSSF

Responses	Frequency	Percentage
Yes	32	40
No	48	60

Table 4.1.5 above summarizes responses about facilities that enable data between datacenter and branch offices to continuously update information to disaster recovery sites. It is indicated that 60% of the respondents rejected and 40 % accepted that at NSSF has remote disk mirroring facilities.

In examining whether NSSF systems undergo disaster simulations to test readiness of automated recovery, the responses collected are shown in the table 4.1.6 below

Table 4.1.7: **Does NSSF carryout regular disaster simulations to test readiness for automated recovery**

Responses	Frequency	Percentage
Yes	27	34
No	53	66

Table 4.1.6 above summarizes responses about the availability of regular disaster simulations at NSSF to test to test readiness for automated business recovery. It is indicated that NSSF systems do not undergo regular drills and disaster simulations to test up-to-datedness of the disaster (66% of the respondents). While 34% of the respondents accepted the view that NSSF systems undergo regular drills and other simulations to test up-to-datedness of the disaster(s).

4.2 Activation Plans at NSSF

In examining how activation plans affect automated business recovery at NSSF, the questions, of the research instrument (questionnaire) were used as an index and the findings collected were tabulated as follows;

Table 4.2.1: Does NSSF have disaster recovery plans available for execution

Responses	Frequency	Percentage
Yes	64	80
No	16	20

Findings in table 4.2.1 above show that 80% of the respondents accept that NSSF has documented disaster recovery plans available. 20% of the respondents reject the view. Further the study sought to establish whether NSSF has a disaster recovery strategic plan that has been endorsed by the minister and the board for implementation and every staff member of NSSF can access it for reference.

The results solicited gathered are herein presented in table 4.2.2 below.

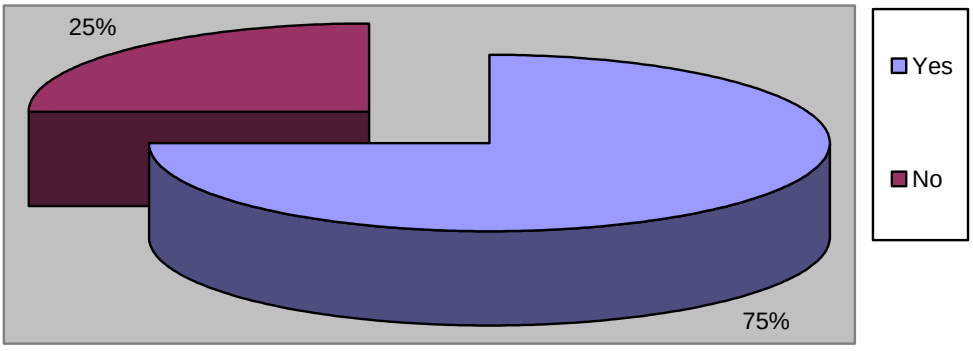
Table 4.2.2: Are there disaster recovery strategic plans at NSSF

Responses	**Frequency**	**Percentage**
Yes	62	78
No	18	22

From the table above, 78% of the respondents indicated that NSSF has a disaster recovery strategic plan that has been endorsed by the minister and the board for implementation and every staff member of NSSF can access it for reference. 22% of the respondents disagreed with the assertion.

In ascertaining whether NSSF has documented disaster simulation and recovery scheme plans the 75% of the respondents answered yes and 25% disagreed. The findings obtained are represented in the graph below (Figure 4.2)

Figure 4.2 Does NSSF have documented disaster simulation and recovery scheme plans



In testing whether NSSF has a disaster recovery and business continuity plan that has been integrated with the corporate management culture, the findings obtained are presented in the table 4.2.3 below.

Table 4.2.3: Are the disaster recovery plans integrated in the corporate culture at NSSF

Responses	Frequency	Percentage
Yes	49	61
No	31	39

From table above the majority (61%) of the respondents accepted that NSSF has a disaster recovery and business continuity plan that has been integrated with the

corporate management culture, as an ongoing activity. It was only 39% of the respondents who rejected the view.

The study also sought to establish whether NSSF has classified and prioritized disaster vulnerabilities, the results collected are shown in the table 4.2.4 below

Table 4.2.4: Has NSSF done a disaster vulnerabilities exercise and carried out a Business Impact Analysis

Responses	Frequency	Percentage
Yes	47	59
No	33	41

The findings in table above Shows that 59% of the respondents were with the view that NSSF has classified and prioritized disaster vulnerabilities and carried out a business impact analysis. The remainder (41%) of the respondents rejected the assertion.

Further using the likert scale of rating respondents where asked to indicated how activation plans influence automated business recovery at NSSF. The findings gathered were tabulated as follow

Table 4.2.5: Activation Plans and Automated Business Recovery in percentages

Activation plans at NSSF	**SA**	**A**	**NS**	**DA**	**SD**
At NSSF system security controls to ensure that resources are used in line with IT policies.	28	40	10	14	8
At NSSF there are system security controls to ensure data integrity and confidentiality.	25	36	12	17	10
At NSSF system security controls to ensure audit trails for critical business data.	23	34	9	20	14

SA- Strongly Agree, A- Agree, NS- Not Sure, DA- Don't Agree, SD- Strongly Disagree

The findings in the table above shows that 68% of the respondents agreed of which 28% strongly agreed that at NSSF, there system security controls to ensure that resources are used in line with IT policies. This implies that at NSSF it policies are properly followed and are clearly displayed and seen in NSSF offices

Further the results in table 4.2.5 Shows that 61% of the respondents agreed of which 25% strongly agreed that at NSSF there are system security controls to ensure data integrity and confidentiality.

In the table 4.2.5 above it was also stated that 64% agree that at NSSF there are system security controls to ensure audit trails for critical business data.

In testing whether there is a relationship between activation plans and automated business recovery in NSSF, the results are shown in the table 4.2.6 below.

Table 4.2.6: Relationship between activation plans and automated business recovery

Table/figure	Responses		Ranks		Out of	Deviation = Ry-Rn	D2
	Yes	No	Ry	Rn			
4.8	64	16	1	5	80	-4	16
4.9	62	18	2	4	80	-2	4
Figure 2	60	20	3	3	80	0	0
4.10	49	31	4	2	80	2	4
4.11	47	33	5	1	80	4	16
$\underline{\Sigma d^2}$							40

Where:-

n = Number of respondents

Ry = Ranks of respondents who said Yes

Rn = Ranks of respondents who said No

d = Difference or deviation between Ry and Rn.

$$R^1 = 1 - \frac{6 \Sigma d^2}{n(n^2 - 1)}$$

$$R^1 = 1 - \frac{6 \times 40}{80(80^2 - 1)}$$

$$= \mathbf{0.99}$$

The findings indicated that there is a high relationship between activation plans and automated business recovery and thus there is a high positive coefficient or rank correlation of 0.99.

4.3 Human Capital and Automated Business recovery at NSSF

In ascertaining how human capital affects automated business recovery at NSSF, the researcher asked the respondents to indicate whether at NSSF, every employee has been sensitized on the organization's disaster recovery strategies. The findings collected are presented in the table as follows

Table 4.3.1: Is there Employee sensitization of organization's disaster recovery strategies

Responses	**Frequency**	**Percentage**
Yes	42	53
No	38	47

The findings in the table above indicates that majority of the respondents (53%) were with a view that every employee has been sensitized on the organization's disaster recovery strategies. Only 47% of the respondents rejected the view that every employee has been sensitized on the organization's disaster recovery strategies.

Further in establishing whether at NSSF there is specialized staff with specialized training to activate DRP/BCP mission critical systems. The findings obtained are herein presented in table 4.3.2 below.

Table 4.3.2: Are there Staff to activate DRP/BCP for mission in critical systems

Responses	Frequency	Percentage
Yes	44	55
No	36	45

Table 4.3.2 above summarizes responses about whether at NSSF there is specialized staff with specialized training to activate DRP/BCP in mission critical systems. 55% of the respondents indicated that at NSSF there is specialized staff with specialized training to activate DRP/BCP mission critical system. While 45% of the respondents rejected the view that at NSSF there is specialized staff with specialized training to activate DRP/BCP mission critical system.

Further using the likert scale of rating respondents where asked to indicated how human capital plans influence automated business recovery at NSSF. The findings gathered were tabulated as follows;

Table 4.3.3: Human capital and automated business recovery at NSSF

Human capital and automated business recovery	**SA**	**A**	**NS**	**DA**	**SD**
NSSF has a disaster recovery and business continuity coordinator	22	36	11	17	14
At NSSF every staff undergo regular disaster simulations	21	37	10	19	13
At NSSF regular fire drills and false alarms are done to test prepared	18	38	14	16	14

SA- Strongly Agree, A- Agree, NS- Not Sure, DA- Don't Agree, SD- Strongly Disagree

From the table4.3.3 above it was noted that 58% of the respondents agree that NSSF has a disaster recovery and business continuity coordinator.

Further the findings in the table 4.3.3 above Shows that majority (58%) of the respondents agreed of which 21% strongly agreed that at NSSF every staff undergo regular disaster simulations like fire drills, false alarms and they know what is expected of them in case of disaster. Also the results in table 4.3.3 reflect that 56% of the respondents agreed of which 18% strongly agreed that at NSSF regular fire drills and false alarms are done to test prepared. This is done to guarantee effective and efficient data security in the Fund. Therefore information administration mechanisms and software are used by the Fund during the fire drills to prove or project the performance and stability to achieve positive results in data and information security.

To determine whether there exists a relationship between human capital and automated business recovery. The findings got are shown in the table below;

Table 4.3.4: Relationship between human capital and automated business recovery

Table/figure	Responses		Ranks		Out of	Deviation = Ry-Rn	D2
	Yes	No	Ry	Rn			
4.3.1	42	38	3	1	80	-2	4
4.3.2	44	36	2	2	80	0	0
4.3.3	54	26	1	3	80	2	4
$\underline{\Sigma d^2}$							8

Where:-

n = Number of respondents

Ry = Ranks of respondents who said Yes

Rn = Ranks of respondents who said No

d = Difference or deviation between Ry and Rn.

$$R^1 = 1 - \frac{6 \Sigma d^2}{n(n^2 - 1)}$$

$$R^1 = 1 - \frac{6 \times 8}{80(80^2 - 1)}$$

$$= 1 - \frac{6 \times 8}{80 \times 6399}$$

$$= 1 - \frac{48}{511{,}920}$$

$$= \mathbf{0.99}$$

The findings indicated that there is a high relationship between human capital and automated business recovery and thus there is a high positive coefficient or rank correlation of 0.99.

4.4 Government Policies and Service Provider Capacity and Automated Business Recovery

4.4.1 Government Policies and Automated Business Recovery

In finding out the modulator effect of government policies on the relationship between factors and automated business recovery, the researcher asked the respondents to indicate whether in Uganda there is legislation by government that requires institutions to provide data and business recovery. The reposes gathered are herein presented in the table 4.4.1 below;

Table 4.4.1: Is there a government policy on data and business recovery

Responses	**Frequency**	**Percentage**
Yes	37	46
No	43	54

As shown in the table above, majority of the respondents (54%) rejected the view that in Uganda there is legislation by government that requires institutions to provide data and business recovery. It was only 46% of the respondents who accepted the view.

In ascertaining whether NSSF usually responds to government audits about her recovery plans in case of a catastrophe or IT related disasters. The responses gathered are shown in the table below

Table 4.4.2: Does Government audit NSSF's business recovery plans

Responses	**Frequency**	**Percentage**
Yes	45	56
No	35	44

According to the results in the table above, 56% of the respondents accepted that NSSF usually responds to government audits about her business recovery plans. 44% did not agree.

In identifying whether the Government provides guidelines through relevant ministries and authorities to public and commercial business entities for implementing and maintaining business recovery programs, the findings obtained are shown in the figure 4.4 below

Figure 4.4: Does Government provide guidelines through relevant ministries to public and commercial business entities for implementing and maintaining business recovery programs

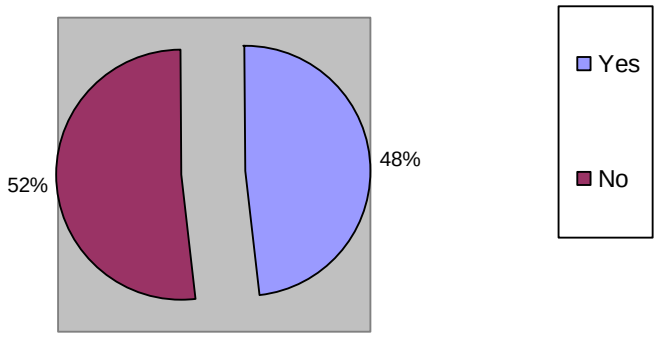


Figure 4.4 above Shows that 52% of the respondents, rejected the view that the Government provides guidelines through relevant ministries and authorities to public and commercial business entities for implementing and maintaining business recovery programs. 48% of the respondents on the other hand agreed with the assertion.

In finding out whether the government has a budget for aiding business entities to recover from disasters. The responses gathered are shown in the table 4.4.3 below

Table 4.4.3: Does Government aid corporate business entities to recover from disasters

Responses	**Frequency**	**Percentage**
Yes	40	50
No	40	50

The results in the table above show that 50% of the respondents accepted that the government has a budget for aiding business entities to recover from disasters. On the other hand 50% of the respondents rejected the view that the government has a budget for aiding business entities to recover from disasters.

In examining whether Business Continuity is part of government's disaster preparedness program, the findings gathered are herein presented in the table as follows

Table 4.4.4: Is Business Continuity part of government's disaster preparedness program

Responses	**Frequency**	**Percentage**
Yes	53	59
No	27	41

From the table above 59% of the respondents were with a view that Business Continuity is part of government's disaster preparedness program. It was only 41% of the respondents who discarded the assertion that Business Continuity is part of government's disaster preparedness program.

4.4.2 Service Provider Capacity and Automated Business Recovery

In establishing the capacity of service providers towards the factors affecting automated business recovery, the researcher asked the respondents to indicate whether various service providers have the capacity to provide data communication services across the country. The findings collected are shown in the table 4.4.5 below

Table 4.4.5: Do Services providers' have enough capacity to provide data communication services across the country

Responses	**Frequency**	**Percentage**
Yes	49	61
No	31	39

The findings in the table above indicates that 61% of the respondents were with a view that various service providers have the capacity to provide data communication services across the country and the minority (39%) indicated that various service providers have no capacity to provide data communication services across the country. Further the findings from the interview also revealed that majority of service providers have demonstrated the capacity to provide enough bandwidth across the whole country. With this assertion therefore, it should be noted that various service providers have the capacity to provide data communication services across the country.

In establishing whether there are data hosting, outsourced DRP programs available to various service providers for client enterprises in Uganda. The findings solicited are herein presented as follow

Table 4.4.6: Are there Data hosting and outsourced DRP programs available from service providers for client enterprises

Responses	**Frequency**	**Percentage**
Yes	50	63
No	30	37

As shown in the table above 63% of the respondents expressed that there are data hosting, outsourced DRP programs available to various service providers for client enterprises in Uganda. The minority (37%) of the respondents rejected the assertion.

In finding out whether the cost of establishing connectivity is regulated and is affordable to most enterprises, the responses got are shown in the table below;

Table 4.4.7: Are costs of establishing connectivity affordable to most enterprises

Responses	**Frequency**	**Percentage**
Yes	39	49
No	41	51

From the table above, majority (51%) of the respondents rejected the view that the cost of establishing connectivity is regulated and is affordable to most enterprises. It was only 49% of the respondents who accepted the view.

In testing whether there exist a relationship between government laws and service provider infrastructure and automated business recovery at NSSF. The results solicited are herein shown in the table below

Table 4.4.8: **Relationship between Government and Service Providers in positioning institutions for automatic business recovery**

Table/figure	Responses		Ranks		Out of	Deviation = Ry-Rn	D2
	Yes	No	Ry	Rn			
4.4.1	37	43	9	1	80	8	64
4.4.2	45	35	5	5	80	0	0
Figure 4.4	38	42	8	2	80	6	36
4.4.3	40	40	6	4	80	2	4
4.4.4	53	27	2	8	80	-6	36
4.4.5	49	31	4	6	80	-2	4
4.4.6	50	30	3	7	80	-4	16
4.4.7	39	41	7	3	80	4	16
$\sum D^2$							174

Where:-

n = Number of respondents

Ry = Ranks of respondents who said Yes

Rn = Ranks of respondents who said No

d = Difference or deviation between Ry and Rn.

$$R^1 = 1 - \frac{6 \Sigma d^2}{n(n^2 - 1)}$$

$$R^1 = 1 - \frac{6 \times 174}{80(80^2 - 1)}$$

$$= \mathbf{0.99}$$

The findings indicated that there is a high relationship between Government Policies and Service Providers in positioning institutions for automatic business recovery and thus there is a high positive coefficient or rank correlation of 0.99.

4.5 Vulnerability and Impact Assessment at NSSF

In identifying factors affecting automated business recovery and in ascertaining the disaster preparedness of an organization and in determining how the occurrences of the disaster affect service delivery in case a disaster arise out of accident, using the scoring system (1- Very Low, 2-Low, 3-Medium, 4-High, 5-Very High), the respondents were asked to tick the most significant factor that can affect service delivery. The findings collected are tabulated as follows

Table 4.5: How the occurrences of the disaster affect service delivery in an organization

Responses	VULNERABILITY (%)					IMPACT (%)				
	Very high	High	Medium	Low	Very Low	Terminal	Devastating	Critical	Controllable	Irritating
Fire outbreak	10	15	30	23	22	5	10	33	30	22
Earthquake	0	5	18	35	42	17	18	15	0	50
Act of Terrorism	2	8	20	31	39	12	32	19	26	11
Act of sabotage	7	11	22	26	34	13	18	20	11	38
Act of war	1	6	19	34	40	43	20	10	0	27
Act of theft	8	18	33	28	13	14	21	30	25	10

Act of labour dispute	2	6	26	38	28	11	26	20	31	12
Loss of power	0	3	12	40	45	1	9	14	46	30
Equipment Failure	10	19	29	20	22	16	23	10	30	21
Act of Hackers or Cyber crime	6	10	31	30	23	13	25	11	29	22
IT systems failure	7	19	29	31	14	33	21	12	20	14
Disclosure of sensitive information	10	17	40	22	11	15	20	31	18	30
Loss of Data or Records	11	19	27	23	20	20	21	18	25	16

As indicated in the table above, the vulnerability of an organization in relation to the occurrence of fire outbreak was moderately ranked with a score of 30%. Further the findings revealed that the impact of fire outbreak towards service delivery was critical with a score of 33%. This implies that organizations have put in place equipments for fire, smoke, suppression and are displayed in all offices. Further warnings messages concerning smoking are clearly displayed and seen in all offices and majority of offices have alarm systems installed. It was also noted that since the impact of fire was critical towards efficient service delivery, organizations have trained staff on how to anticipate and respond to indicators fire out break.

Further the findings from the table 4.5 above shows that the vulnerability of an organization in relation to the occurrence of earthquake was ranked as very low with a score of 42%. Further the findings revealed that the impact of earth quake towards service delivery was irritating with a score of 50%. This is because there are no incidences of earthquakes and these affect the smooth running of the business.

From the table 4.5 above, it is reflected that the vulnerability of an organization in relations to the occurrence of acts of terrorism was ranked very low with a score of 39%. This implies that organizations have put security measures in place such as metal detectors, security guards among others to prevent terrorism acts. Further it was highlighted that since terrorism acts are precarious towards efficient service delivery, its impact was devastating with the score of 32%

The findings in table 4.5 also show that the vulnerability of an organization in relation to the occurrence of acts of sabotage was ranked very low with a score of 34%. And its impact towards efficient service delivery was irritating with a score of 38%. This is because when an organization has put in place security systems such as firewall, limited access to IT systems this reduces the chances for information sabotage and in case information links out the organization is very minimal to cause catastrophe towards efficient service delivery.

As shown in the table 4.5, the vulnerability of an organization in relation to the occurrence of acts of war was ranked very low with a score of 40%. However, since acts of war cripples the performance of many organization, its impact towards services delivery war terminal with a score of 43%

The results in table 4.5 revealed that the vulnerability of an organization in relation to the occurrence of acts of theft was moderately ranked with a score of 33%. The impact of theft in relation to efficient service delivery was critical with a score of 30%. This is because there are physical control measures in place and sensitive areas are well protected to limit unauthorized people from accessing or reaching such area.

From the table 4.5, the vulnerability of an organization in relation to the occurrence of acts of labour dispute was ranked low with a score of 38%. Further it was highlighted that since acts of labour disputes can in most cases be resolved amicably, its impacts towards efficient service delivery, it impact was controllable with the score of 31%

It is reflected in table 4.5 that the vulnerability of an organization in relation to loss of power or water was ranked very low with a score of 45%. This is because the organization has standby generator to overcome the disaster of loss of power which can cripple smooth execution of tasks. Therefore, the impact of loss of power towards efficient service delivery was controllable with a score of 46%.

From the table 4.5 the vulnerability of an organization in relation to Equipment failure was moderately ranked with a score of 29%. This is because the organization rarely experience equipment failure as most of the equipments are serviced and repaired on regular basis to enhance business continuity. Therefore, the impact of equipment failure towards efficient service delivery was controllable with a score of 30%. Although if not acted on immediately it can result into loss of production and financial control systems, costs run out of control and cash flow goes into reverse as creditors seek immediate payment and debtors defer settling bills knowing that credit control systems are not available to purse them.

Further more, the findings in table 4.5 vulnerability of an organization in relation to the occurrence of act of hackers or cyber crime was moderately ranked with a score of 31%. Further the findings revealed that the impact of cyber crime towards service delivery was controllable with a score of 29%. This implies that organizations have put in place data security systems such as firewalls, internet proxying, access controls lists in routers and switches to protect the organization's data from the computer hackers.

The vulnerability of an organization in relation to the occurrence of IT systems failure was moderately ranked with a score of 29%. The findings revealed that the impact of IT systems failure towards service delivery was devastating with a score of 33%. This implies that most organizations place much emphasis on IT systems because in of IT system failure this forces existing customers to transfer business elsewhere, and prospects may not be converted into new customers and that the new business is strangled; even loyal customers can quickly become dissatisfied.

Chapter 5

SUMMARY, DISCUSSION,CONCLUSION&RECOMMENDATIONS

5.1 Introduction

The study set out to examine factors affecting automated business recovery at the National Social Security Fund. This chapter comprises of summary of findings, a discussion of findings, lessons learnt from the study and recommendations of the study which should be put into practice in order to enhance automated business recovery at the Fund and in other organisations where business recovery and business continuity cannot be ignored or delayed.

5.2 Summary

The research examined how recovery facilities, activation plans and human capital affect automated business recovery at National Social Security Fund. The study found that NSSF has instituted some recovery facilities to protect data but these facilities are not sufficient enough to trigger automated business recovery. There are also documented disaster recovery plans in place but these were only seen in administration and only for disasters like fire. No documented activation plans were found in Information Systems Department which plays a key role and should be a driver for automated business recovery. NSSF has trained some staff in business continuity and disaster recovery planning, it also have some members of staff that have certified competences in Business Continuity Management and Information Security Management as well. This should position better for implementation of automated business recovery if other factors are adequately provided for. Much as government does not aid disaster recovery. From the study, it is revealed that there is enough capacity from service providers to offer enough capacity for business to

implement business recovery strategies including providing infrastructure, and actual recovery facilities. This is sufficient enough therefore, for NSSF to initiate and implement an automated business recovery and answer to the Government's call advise in order not leave the members money in exposure.

Lastly, the study found that in Uganda, there is no legislation by government that requires institutions to provide data and business recovery.

5.3 Discussion

5.3.1 Recovery Facilities

As NSSF business continues to grow, so will be its data and data center requirements in terms of both size and complexity. Data centers are expensive to run, maintain, in terms of staff and infrastructure how the value of the data to be protected exponentially supersede all these costs. For an organisation to run efficiently and effectively, it must run on and maintain reliable data form a well managed information system in order to provide quality service to her clients. Information systems are vulnerable to a number disasters including fire, hacking, thefts, loss of power, IT systems failure, equipment failure, loss of data and records, social engineering acts etc and all these can be catastrophic if not well guarded against. NSSF has tried to put in place programs to guard against these vulnerabilities through installation of fire depressants to depress fire out breaks, antivirus to prevent virus from harming and corrupting data, access controls to prevent unauthorised access and track ingress and egress to the data centre. It has also invested in robust power backup system to ensure that the data centre has clean and constant power supply all the time. NSSF has an information system backup solution with well documented polices and procedures, which ensures that all data is backed up and stored in safe place out side

the metropolitan area of the data centre operations. This backup solution uses tapes that are store in fire proof safes and are recycled when full. This is the cornerstone for any systems recovery at the fund. It was also discovered that no major catastrophe concerning data and the information systems in general has occurred at the fund so as to warrant a full-size system recovery. No record of recovery test results were found as well! Despite this pseudo comfort, the tape backup system has a number of shortfalls, first of all data between backups is vulnerable, for example, if one's last backup was midnight and the storage system failed in the afternoon, any data created during the several hours between the last backup and the hardware failure event is lost. Secondly tapes are very small devices (almost the size of a matchbox) and mobile this makes them liable to getting lost an incident that can lead to information loss or disclosure of sensitive data. They are also prone to many environmental hazards like heat, magnetic fields, water spillages which once exposed to causes them to fail. Baltazar (2003) asserts that the problem with tape backup can be solved using data replication where data can be moved and synchronized between primary and backup sites in short amount of time, thereby guaranteeing business continuity in case of disaster hence data and information security. The study revealed that these services are available within Uganda as outsourced recovery or data centres from reputable service providers or NSSF can as well consider building and operating its own disaster recovery site with automated business recovery functions. Either way trends show that the costs for bandwidth (network connectivity) is steadily reducing due to the advent of fibre connectivity recently acquired by Uganda and the increasing number of service providers in this field.

Outsourced data centres are becoming more affordable, because they lift much of the heavy responsibility from the business. When organizations place their trust in an off-

site data center, they do not need to shoulder this burden alone.

A high availability data center that is automated business recovery capable will place a great deal of emphasis on the following:

Skilled IT Professionals: A data center is only as good as its staff. Security and networking teams need to be well-trained, skilled, and experienced. Network technicians need to be trained to the highest industry standards.

Proper Environment: The environment of a data center is of the utmost importance. There must be an uninterruptible power supply or backup generator, a highly sensitive HVAC system to filter air, a fire suppression system, and proper installation of equipment.

High Level of Security: Data needs to be protected, and the first level of defense is the physical security of the building. There should be controlled access, video surveillance, and extensive employee background checks.

Top of the Line Equipment: Network infrastructure is one of the most important aspects of data center planning. When selecting a data center, make sure equipment selection and infrastructure set-up receive the emphasis they deserve.

Strict Adherence to Standards: Industry standards are around for a reason. They help make sure data centers provide high quality service, maximum availability, and top-shelf security measures.

5.3.2 Activation plans at NSSF

Much as the study asserts that at NSSF there are disaster activation plans in place, these are just fire management procedures and not complete business recovery activation plans. These available include: documented procedures for fire prevention, detection and suppression procedures and are well displayed in all offices. A

comprehensive business recovery plans ought to be made that is guided by a business impact analysis and a constructive assembly of all recovery strategies that these plans must drive. Once developed, NSSF should have them endorsed and approved by the top leadership and incorporate them into the organisation's management culture. These plans should be dynamic and updated regularly. Disaster simulations that are done biannually should help in determining their up-to-datedness and their reliability.

5.3.3 Human Capital and Automated business recovery at NSSF

The study finds that The National Social Security Fund has key competences in business continuity and is continuing to develop staff by through training in areas of disaster and risk management. At the time of the study, the IT department had started on an internal capacity building program by building redundant systems and simulating disaster situations. At the same time, the risk department was championing an enterprise wide business impact analysis. All these are key processes in the implementation of automated business recovery solutions. Management has put up a business continuity steering committee to spearhead all business continuity development activities and this is a right step in achieving automated business recovery. It is among others charged with the responsibility of developing a business impact analysis, formulating business recovery strategies, documenting recovery activation plans and nominating a business continuity response team for top management's approval.

5.3.4 Modulator effect of Service Providers and Government Policies

Much as there was no formal, documentation and policy framework on Government's guidance for institutions to implement disaster recovery plans like it is in Australia, USA, UK and other developed economies, it is apparent that supports growth and

sustainability if digital/business in Uganda. The Ministry of Disaster Preparedness and that of Information and Communication Technology are currently engaged in the process of instituting a national task force that will guide corporations, ministries, parastatals etc to develop and manage business continuity programs. From document analysis, it was discovered that Uganda has launched a US$ 30 million (approximately Shillings 68 billions) National Data Transmission Backbone Infrastructure (NBI) and Electronic Government Infrastructure (EGI) project. The NBI is intended to ensure that affordable high bandwidth data connection is available in all major towns of the country by 2010. The EGI is designed to refurbish government communication infrastructure and reduce the cost of doing electronic business in Uganda (Ladu, 2009). This finding implies that government is both directly and directly interested in electronic business continuity through establishment of an enabling environment.

Not only that, It was also found that NSSF usually responds to government audits about her recovery plans in case of a catastrophe or IT related disasters. In cross examination of the Fund's IT reports, it was discovered that The Central Bank which is currently the regulator of the Fund on behalf government in 2004 contracted PKF consulting Ltd to conduct an audit and make opinions on the IT systems at NSSF. The business recovery and business continuity were part of the scope an implication that government is concerned about her recovery plans in case of a catastrophe or IT related disasters.

Further the findings from the interview revealed that in Uganda legislation is underway to enforce institutions to provide data and business recovery. In a discussion with the Minister of Disaster Preparedness and Relief revealed that the

legislation was in its infancy stage. He decried at how we focus on other disasters like famine, flooding and associated relief aid and yet little attention is given to high risk institutions that drive or govern the economic stability of the country.

The Minister for Disaster Preparedness, affirmed that the ministry has already engaged a consultant to draft Disaster Preparedness Strategy and Policy framework that would in turn provide for legislation. Because there is no legislation some organizations may not bother in investing in disaster recovery and business continuity strategy because of lack of compliance laws and enforcement in the country. With this finding, it should be argued that unless compliance laws are put in practice, many organizations may not invest in disaster recovery to enhance maximum storage, data protection, increase storage facilities as this constraint organizational budget.

5.4 Conclusion

In conclusion, the study has established that all other impediments and shortcomings notwithstanding, NSSF has endeavored and is continuing to put in place disaster management strategies but these are still spotty and insufficient to produce an automated business recovery. In the area of human capital, NSSF is well positioned, to manage and sustain an automated business recovery program but still has a lot to do in acquiring the necessary recovery facilities first as discussed in this chapter. Activation plans are a documented derivative of reliable recovery facilities and skilled human capital activities and process flow management. It can also be argued that the absence of an effective business recovery program at NSSF continuity as a result of lack of a stringent government legislation that requires institutions to provide and implement sound business resumption and continuity programs.

5.5 Recommendation

The key challenge of business continuity preparation is not technology, but the internal marketing "business" aspects such as, justification for a business continuity project, executive buy-in, broad organizational support, and governance and politics.

It is therefore recommended that NSSF should sensitize all staff about the dangers of disasters, their causes and the benefits of having a business continuity plan incase disasters strike. It should also continue a lot more on disaster prevention. NSSF should prioritise an immediate acquisition of an enterprise wide disaster recovery plan to cover; immediate reaction procedures, restoration of the computing infrastructure, restoration of the applications, resumption of business processing under emergency arrangements and restoration of the primary computing service. This would guarantee continued service delivery and reposition NSSF more firmly to stand the impending liberalisation. Further, NSSF should ensure that there is maximum security of data and information as first step towards disaster recovery. This is because client's trust of an organization among others depends on having data and information that is reliable. Effective and efficient data and information security is a cornerstone in implementing sustained disaster recovery/business continuity projects.

Bibliography / References

Bandyopadhyay, K (2001). The Role of Business Impact Analysis and Testing in Disaster Recovery Planning by Health Maintenance Organizations. *Hospital Topics,* 79(1), Winter 2001, 16-21.

Bandyopadhyay, K., & Schkade, L. (2004). Initiation, Adoption, and Implementation of Disaster Recovery Planning by Health Maintenance Organizations. *International Journal of Internet and Enterprise Management*, 2(4), 2004, 309-340.

Botha, J., &VonSolms, R. (2004). A Cyclic Approach to Business Continuity Planning. *Information Management & Computer Security*, 12(4), 2004, 328-337.

Business Continuity Institute, *BCI (2005).* Business Continuity Research Report 2005. Retrieved from http://www.thebci.org/BCIResearchReport.pdf, June 9, 2005.

Calderon, T.G., & Dishovska, M. (2005). Transitioning From Disaster Recovery Management to Business Continuity Management. *Internal Auditing*, Mar/Apr 2005, 21-28.

Cerullo, V., and Cerullo, M.J. (2004). Business Continuity Planning: A Comprehensive Approach. *Information Systems Management*, 21(3), summer 2004, 70-78.

Chow, W. S.(2000). Success Factors for IS Disaster Recovery Planning in Hong Kong. *Information Management & Computer Security*, 8(2), 2000, 80-87.

Clarke, L.(2004). What's The Plan: A Conversation with Lee Clarke. *Harvard Business Review*, June 2004. Deloitte, *2004 Global Security Survey.*

DeSimone, A. J., &Morris, P.(2003). Continuity Planning Now More Critical Than Ever. *American Banker*, 168(50), March 14, 2003, 6.

Das, A. (1997). Determinants of Computer Security Practices**.** *Proceedings of the Americas Conference on Information Systems, 1997*, retrieved from all.net/books/iw/iwarstuff/hsb.baylor.edu/ ramsower/ais.ac.97/papers/das.htm.

DiMartini, W. P.(1996). What Drives Contingency Planning- The Carrot or the Stick? *Contingency Planning & Management*, March 1996, 15-19.

Douglas, P. (1999). Disaster business continuity: promoting staff capability: Disaster Prevention and Management", 8(2):127–133, 1999.

Eklund, B.(2001), "*Business Unusual*", netWorker, Vol. 5, Iss. 4, pp. 20-25.

Eschellbeck, G. (2000). Active Security- A Proactive Approach for Computer Security Systems. *Journal of Network &Computer Applications*, No. 23, 2000, pp.109-130.

Ernest & Young (2004). Global Information Security Survey*, 2004.*

Falconer, D. J., &Hodgett, R. A. (1999). Why Executives Don't Respond to Your Survey. *Proceedings of the 10 Australasian Conference on Information Systems*, Wellington, New Zealand, 1 – 3 December 1999, 279-285.

Flood, S. (2005). There's No Full Stop in Disaster**.** *Computer Weekly*, May 3, 2005, 34-35.

Fulford, H., &Doherty, N.F.(2003). The Application of Information Security Policies in Large UK-Based Organizations: An Exploratory Investigation. *Information Management & Computer Security*, 11(3), 2003, 106-114.

Hecht, J. A. (2002). Business Continuity Management. *Communications of the*

AIS, 8, 2002, 444-450.

Heller, 2004?

Hiles, A. (1992). Surviving a Computer Disaster**.** *Engineering Management Journal*, Dec. 1992, pp. 271-274.

Louderback, J. (1995). Will You Be Ready When Disaster Strikes?" *PC Week,* 12(5), February 6, 1995, 130.

McFarlan, F.W., McKenney, J.L., & Pyburn, P.(1983). The Information Archipelago-

Plotting the Course. *Harvard Business Review*, January-February 1983, 145-155.

Mitroff, I.I., & Alpaslan, M.C.(2003). Preparing For Evil.

Harvard Business Review, 81(4), April 2003, 109-115.

Mitroff, I.I., Harrington, L.K., & Gai, E.(1996). Thinking About the Unthinkable.

Across the Board, 33(8), Sept 1996, 44-48

Nemzow, M.(1997). Business Continuity Planning**.** *International Journal of Network Management*, Vol. 7, 1997, pp. 127-136.

Nunnally, J.L. (1979). Psychometric Theory. McGraw-Hill, New York, 1979.

Pearson, C.M. &Clair, J. A. (1998). Reframing Crisis Management**.** *Academy of Management Review*, 23(1), 1998, 59-76.

Appendix 1

Instrument 1 - Questionnaire

Factors affecting automated business recovery at National Social Security Fund, Uganda

Introduction

Dear respondent, I am Immy Byaruhanga**,** a Masters Degree student at Uganda Management Institute (UMI) who is carrying out an academic study on Factors affecting automated business recovery at National Social Security Fund, Uganda. You are humbly requested to volunteer and answer the questions in this questionnaire. The study is entirely for academic purposes and any information given will be treated with utmost confidentiality.

Thank you for your cooperation.

Research Instrument 1(This research instrument is meant for members of staff at NSSF)

In the questions below, please tick or fill in what is most appropriate to your.

Section A: Recovery Facilities

1. Has NSSF outsourced recovery services from commercial hot sites, or cold sites for the purpose of automating business recovery ?

   Yes ☐ No ☐

2. a) Do you think NSSF has data storage facilities such as tapes disks, CDS with up-to date information as back-up facilities?

   Yes ☐ No ☐

   b) Please support your answer…….

3. Do you think at NSSF there is Backup and off-site storage of mission critical data a facility otherwise known as a disaster recovery centre?

   ☐ ☐

Yes No

4. Do you think NSSF does electronic vaulting where data is stored at a secondary site as a fall back in case of a disaster?

   Yes ☐ No ☐

5. Are there Redundant or backup links between data centre and branch offices

   Yes ☐ No

   b) Please support your answer…….

6. Does NSSF have remote disk mirroring facilities that enable data from all NSSF branch networks to continuously update information to disaster recovery sites?

   ☐

   Yes ☐ No

7. Does NSSF carryout regular disaster simulations to test readness for automated recovery?

   Yes ☐ No ☐

Section B: Activation Plans

8. a) Do you think NSSF has documented disaster recovery guidelines and all employees are aware of them?

   Yes ☐ No ☐

   b) Please support your answer……

9. a) Is there a disaster recovery strategic plan that has been endorsed by the top management and staff member of NSSF can access it for reference?

   Yes ☐ No ☐

   b) Please justify your answer……

10. Is there a routine disaster simulation and recovery schemes at NSSF whose results were published?

    Yes ☐ No ☐

11. a) Do you think NSSF has a disaster recovery and business continuity plan that has been integrated with the corporate management culture, as an ongoing activity?

    Yes ☐ No ☐

    b) Please justify your answer……

12. Has NSSF classified and prioritized disaster vulnerabilities?

    Yes ☐ No ☐

13. At NSSF, there is monitoring and maintaining how resources are used in line with IT policies.

    5. Strongly agree 4. Agree 3.Not sure 2. Disagree 1.Strongly disagree

14. At NSSF when there is Termination of employment (access privileges removed), the employees username and password is eliminated immediately.

5. Strongly agree 4. Agree 3.Not sure 2. Disagree 1.Strongly disagree

15. At NSSF, audit trails exist in critical business data can reflect a username who made changes, time the changes were made and particulars that were changed.

5. Strongly agree 4. Agree 3.Not sure 2. Disagree 1.Strongly disagree

Section C: Human Capital

16. Has NSSF sensitized every employee on the organization's disaster recovery strategies? Yes ☐ No ☐

17. Are there specialized staff with specialized training to activate DRP/BCP mission critical systems at NSSF?

Yes ☐ No ☐

18. Are NSSF staff trained on how to anticipate and respond to indicators of disaster like fire, earthquakes, strikes, war, scarcity, etc?

Yes ☐ No ☐

19. NSSF has a disaster recovery and business continuity coordinator.

5. Strongly agree 4. Agree 3.Not sure 2. Disagree 1.Strongly disagree

20. At NSSF every staff undergo regular fire drills, false alarms and they know what is expected of them in case of disaster.

5. Strongly agree 4. Agree 3.Not sure 2. Disagree 1.Strongly disagree

21. At NSSF regular fire drills and false alarms are done to test prepared

5. Strongly agree 4. Agree 3.Not sure 2. Disagree 1.Strongly disagree

Section D: Government Policies / Laws and Service Provide infrastructure

22. Is there legislation in Uganda that requires institutions to provide data and business recovery?

Yes ☐ No ☐

23. Does NSSF usually responds to government audits about her recovery plans in case of a catastrophe or IT related disasters?

Yes ☐ No ☐

24. a) Do you think the Government provides guidelines through relevant ministries and authorities to public and commercial business entities for implementing and maintaining business recovery programs?

Yes ☐ No ☐

b) Please support your answer……..

25. Do you think the government has a budget for aiding business entities to recover from disasters?

Yes ☐ No ☐

26. Do you think Business Continuity is part of government's disaster preparedness program?

Yes ☐ No ☐

27. Do service providers have capacity to provide data communication services across the country?

☐ ☐

Yes No

28. Are there data hosting, outsourced DRP programs available to various service providers in for client enterprises in Uganda to ensure smooth business recove

Yes No

29. Is the cost of establishing connectivity regulated and affordable to most enterprises?

Yes No

30. Has NSSF implemented data security systems such as, firewalls, access control lists in routers and switches, internet proxying, etc?

Yes No

Thank you for your participation

Apendix 2

Research Instrument 2

In the questions below, please write/ tick the appropriate corresponding answer.

Qn1. Level of decision making in the organization: *tick the appropriate*

3. Middle management 2.Senior Management 1. Board of Directors

Qn2. My current experience bias is in: ***tick the appropriate***

1) Corporate Governance
2) Financial Management
3) Information Management
4) General Management

Qn3. Experience in the above work strata ***tick the appropriate***

1) Less than 1 year
2) 1- 5 years
3) 5-10 years
4) More that 10 years

Qn4. Has organization implemented any disaster recovery strategies?

a) Yes b) No

Qn5. If no, why has your organization not implemented any disaster recovery strategies?

I. ……
II. ……

Qn6. If yes**,** what business resumption strategy has been implemented in your organization (tick appropriately)

I. Cold Site,
II. Hot Site
III. Tape backup, CDS, etc
IV. Remote disk mirroring facilities
V. Electronic vaulting

VI. Organized manual procedures

VII. Others- specify

Qn7. In your opinion, are the above strategies sufficient for your organization to recover and automatically resume business from any disruption caused by a disaster?

5. Strongly agree 4. Agree 3.Not sure 2. Disagree 1.Strongly disagree

Qn8. In this section, make your own rating of the probability as well as the impact on your organization service delivery in case of suffering a disaster arising out of the following incidents by ticking appropriately:

a) Fire outbreak

Vulnerability level

1. Very high 2. High 3. Medium 4. Low 5. Very Low

Impact rating

1. Terminal 2. Devastating 3. Critical 4. Controllable 5. Irritating

b) Earth quake

Vulnerability level

1. Very high 2. High 3. Medium 4. Low 5. Very Low

Impact rating

1. Terminal 2. Devastating 3. Critical 4. Controllable 5. Irritating

c) *Act of Terrorism*

Vulnerability level

1. Very high 2. High 3. Medium 4. Low 5. Very Low

Impact rating

1. Terminal 2. Devastating 3. Critical 4. Controllable 5. Irritating

d) Act of Sabotage

Vulnerability level

1. Very high 2. High 3. Medium 4. Low 5. Very Low

Impact rating

1. Terminal 2. Devastating 3. Critical 4. Controllable 5. Irritating

e) *Act of War*

Vulnerability level				
1. Very high	2. High	3. Medium	4. Low	5. Very Low
Impact rating				
1. Terminal	2. Devastating	3. Critical	4. Controllable	5. Irritating

f) *Act of Theft*

Vulnerability level				
1. Very high	2. High	3. Medium	4. Low	5. Very Low
Impact rating				
1. Terminal	2. Devastating	3. Critical	4. Controllable	5. Irritating

g) *Act of Labour dispute*

Vulnerability level				
1. Very high	2. High	3. Medium	4. Low	5. Very Low
Impact rating				
1. Terminal	2. Devastating	3. Critical	4. Controllable	5. Irritating

h) Loss of Power or water

Vulnerability level				
1. Very high	2. High	3. Medium	4. Low	5. Very Low
Impact rating				
1. Terminal	2. Devastating	3. Critical	4. Controllable	5. Irritating

i) Equipment Failure

Vulnerability level				
1. Very high	2. High	3. Medium	4. Low	5. Very Low
Impact rating				
1. Terminal	2. Devastating	3. Critical	4. Controllable	5. Irritating

j) *Act of Hackers or Cyber crime*

Vulnerability level				
1. Very high	2. High	3. Medium	4. Low	5. Very Low
Impact rating				
1. Terminal	2. Devastating	3. Critical	4. Controllable	5. Irritating

k) *IT systems failure*

Vulnerability level

1. Very high 2. High 3. Medium 4. Low 5. Very Low

Impact rating

1. Terminal 2. Devastating 3. Critical 4. Controllable 5. Irritating

l) Disclosure of sensitive information

Vulnerability level

1. Very high 2. High 3. Medium 4. Low 5. Very Low

Impact rating

1. Terminal 2. Devastating 3. Critical 4. Controllable 5. Irritating

m) *Loss of Data or Records*

Vulnerability level

1. Very high 2. High 3. Medium 4. Low 5. Very Low

Impact rating

1. Terminal 2. Devastating 3. Critical 4. Controllable 5. Irritating

Qn11. what are the major hazards that affect organizations?

i. ……
……

ii. ……
……

Qn12. What factors make the organization vulnerable?

i. ……

ii. ……

Qn13. What are the most effective mitigation strategies?

i. ……

ii. ……

Qn14. What do you consider as success factors for implementing disaster recovery or business continuity plan?

i. ……

ii. ……

<u>Thank you for your participation</u>