Nigeria 2006-11013A

PUBLIC VERSION

THE Nigerian STOCK EXCHANGE

Nigerian Stock Exchange (NSE) Business Continuity Plan (BCP) & Disaster Recovery Plan (DRP)

FINAL REPORT

RECEIVED
AUG 19 2010
U.S. TRADE AND DEVELOPMENT AGENCY

1 copy Public

GS RB
JW AM
PD NG
DD PM
DR
DE

Prepared by:

Global Information Technology, Inc. (GIT)
Tampa Florida, USA

June 2010

This report was funded by the U.S. Trade and Development Agency (USTDA), an agency of the U.S. Government. The opinions, findings, conclusions, or recommendations expressed in this document are those of the author(s) and do not necessarily represent the official position or policies of USTDA. USTDA makes no representation about, nor does it accept responsibility for, the accuracy or completeness of the information contained in this report.

Mailing and Delivery Address: 1000 Wilson Boulevard, Suite 1600, Arlington, VA 22209-3901
Phone: 703-875-4357 • **Fax:** 703-875-4009 • **Web site:** www.ustda.gov • **email:** info@ustda.gov

THE U.S. TRADE AND DEVELOPMENT AGENCY

The U.S. Trade and Development Agency (USTDA) advances economic development and U.S. commercial interests in developing and middle income countries. The agency funds various forms of technical assistance, early investment analysis, training, orientation visits and business workshops that support the development of a modern infrastructure and a fair and open trading environment.

USTDA's strategic use of foreign assistance funds to support sound investment policy and decision-making in host countries creates an enabling environment for trade, investment and sustainable economic development. Operating at the nexus of foreign policy and commerce, USTDA is uniquely positioned to work with U.S. firms and host countries in achieving the agency's trade and development goals. In carrying out its mission, USTDA gives emphasis to economic sectors that may benefit from U.S. exports of goods and services.

Mailing and Delivery Address: 1000 Wilson Boulevard, Suite 1600, Arlington, VA 22209-3901
Phone: 703–875–4357 • **Fax:** 703–875–4009 • **Web site:** www.ustda.gov • **email:** info@ustda.gov

Mailing and Delivery Address: 1000 Wilson Boulevard, Suite 1600, Arlington, VA 22209-3901
Phone: 703–875–4357 • **Fax:** 703–875–4009 • **Web site:** www.ustda.gov • **email:** info@ustda.gov

Table of Contents

EXECUTIVE SUMMARY **7**

INTRODUCTION **9**

- BACKGROUND 9
- OBJECTIVES 9
- SCOPE OF THE EFFORTS 10
- KEY STAKEHOLDERS 10
- READER GUIDE AND DOCUMENT SUMMARY DESCRIPTION 11
- DR BCP ACRONYMS AND GLOSSARY OF TERMS 18

GIT WORK APPROACH **22**

- ASSESSMENT AND EVALUATION 22
- DR DATA GATHERING & CURRENT STATE ASSESSMENT 23
- CSA DATA ANALYSIS AND SCORING 24
- DR FACILITY PLAN, PROCEDURES & SPECIFICATIONS REPORT PROJECT STEPS 24
- FACILITY & SPECIFICATION REPORT PREPARATION 25

NSE CURRENT STATE ASSESSMENT (CSA) **26**

- CURRENT NSE ENVIRONMENT - ASSESSMENT 26
- NSE EMERGENCY RESPONSE PROCEDURES - ASSESSMENT 29
- NSE DR PLAN ACTIVATION PROCEDURES - ASSESSMENT 31
- NSE ADMINISTRATIVE PROCEDURES - ASSESSMENT 33
- NSE DR REPORTS AND FORMS - ASSESSMENT 38

DR STRATEGIC NEEDS & SYSTEM SPECIFICATIONS **41**

- HARDWARE & SOFTWARE SPECIFICATIONS 41
- DR FACILITY SPECIFICATIONS 41
- DOCUMENTED GENERAL & TECHNICAL SPECIFICATIONS. 42
- REDUNDANCY NEEDS 43
- SERVICE LEVEL AGREEMENT (SLA) EXPECTATIONS. 45
- NETWORKING, CONNECTIVITY AND CIRCUITS. 47
- POWER CONSUMPTION. 49
- COOLING CAPABILITIES. 50
- FIRE PROTECTION. 51
- DATA REPLICATION. 53
- SITE PLAN. 54

IMPLEMENTATION PLAN **55**

- TASK & DELIVERABLE SUMMARY 55
- NSE WORK PLAN DETAILS 55
- IMPLEMENTATION PLAN EFFORT ESTIMATES AND SCHEDULE 55
- PREMISES & ASSUMPTIONS 56
- ROLES AND RESPONSIBILITIES 57
  - *Market Operations Related* *57*
  - *Risk Management & Regulation Related* *57*
  - *Information Technology & Market Operations Related* *59*
  - *HR & Real Estate Related* *59*

NSE SUPPLIERS AND IMPACT RESULTS **60**

SUPPLIER IDENTIFICATION 60
Nigerian Suppliers 60
United States Suppliers 61
DEVELOPMENT IMPACT ANALYSIS 62
DEVELOPMENT BENEFITS ANALYSIS 63
Security Benefits 63
Reliability Benefits 64
Data Integrity Benefits 64
Other Benefits 64
PROJECT BENEFIT ESTIMATE 65
Infrastructure I Industry 65
Market-Oriented Reforms 65
Human Capacity Building 66
Technology Transfer and Productivity 66
Other. 67

APPENDIX **68**

1. NSE BCP/DRP PROJECT QUESTIONNAIRE 70
2. LETTER OF INVITATION 91
3. NSE NETWORK DIAGRAMS AND RESOURCES 92
NSE Hardware and Resources 92
NSE Interconectivity and Network 93
NSE IT Infrastructure 94
4. NSE BCP/DRP DISASTER AND CONTINGENCY PLAN PROCESS 95
Project Initiation Phase 96
Business Impact Analysis Phase 97
Strategy Selection Phase 98
Documentation Of Minimum Resource Requirements (Detail) 99
Plan Preparation Phase 100
Testing And Maintenance Phase 101
5. DECISIONS RELATED TO FAILOVER VS. BACKUP 102
6. NSE EMERGENCY TEAM COMPOSITION 106
Emergency Management Team (EMT) 106
7. NSE RESOURCES 108
Software Resources: 108
Server Hardware Resources: 108
End User Hardware: 108
Telecommunications Resources: 108
NSE Interconectivity and Network 109
NSE IT Infrastructure 110
8. NSE IMPLEMENTATION PLAN 111
9. NSE BCP STANDARDS 122
BC/DR Planning Related 122
BC/DR Recovery and Restoration Factors Related 123
BC/DR Testing Related 124
BC/DR Quality and Control Related 125
BC/DR Staff Related 126
10. NSE BCP PLAN, EMERGENCY ACTIONS & PROCEDURES 127

Procedure Overview *127*
Emergency Mobilization *133*
Emergency Procedures *135*
Team Action Plans *139*
Emergency Phase Procedures *141*
Recovery Phase Procedures *142*
Restoration Phase Procedures *142*
Notification Team Procedures – All Phases *145*
Testing and Maintenance *148*
Event and Situation Triggered Reviews and Actions *149*
Forms, Checklists & Reports *157*
11. NSE DISASTER RESPONSE & RECOVERY PROCEDURE & CHECKLISTS 162
Emergency Contact Form & Procedure *162*
Emergency Procedures & Instructions *164*
Restoration Actions & Procedure *167*
Recovery & Completion Procedures *171*
12. SAMPLE - NSE DISASTER RECOVERY PROCEDURE GUIDE 173
Emergency Levels *176*
Emergency Response Team Actions & Instructions *178*
Hazards and Threat Profiles and Actions *182*
Alternate Site Configuration and Checklists *188*
13. SAMPLE MUMBAI DRP 195
14. NSE SUPPLIER AND IMPACT QUESTIONNAIRE AND RESPONSE 228
15. THE NIGERIAN STOCK EXCHANGE PROPOSED ORGANIZATION PLAN & CHARTS 237
Appedix Details begin on Next Page *237*
16. NSE BCP/DRP PROJECT QUESTIONNAIRE RESPONSE 238
Appedix Details begin on Next Page *238*
17. GIT NSE DRP PROPOSAL FOR TECHNICAL ASSISTANCE 239
Appedix Details begin on Next Page *239*
18. NSE ORIGINAL ANALYSIS 240
Appedix Details begin on Next Page *240*

EXECUTIVE SUMMARY

The Nigerian Stock Exchange (NSE) was established in 1960. The NSE and its management team understand the importance of a reliable stock exchange and requested the U.S. Trade and Development Agency (USTDA) provide "Technical Assistance" to facilitate development of a Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP).

Global Information Technology, Inc. (GIT) was awarded the contract to provide the services necessary to develop a DRP for the NSE on November 11, 2008. The project was funded in it's entirety by the USTDA.

GIT received funding and began phase one of this project in February 2, 2009 and assembled a team on the ground in Lagos, Nigeria to:

- Begin acquisition of the information and data necessary to develop the plan
- Evaluate and develop a Current State Assessment (CSA) of the NSE DRP & BCP data
- Prepare and document the Gap Analysis compared to Industry Best Practices.

Initially a review and assessment of the current state of information was conducted that led to a number of conclusions and consequential recommendations.

- A significant number and percent of areas (over 80%) were Missing and undocumented as shown in the summary table below.
- NSE requires completion of extensive documentation and support procedures in order to establish a successful, testable and maintainable DRP.

RATING CRITERIA	COLOR	COUNT	PERCENT
GREEN = MEETS ALL CRITERIA		2	4%
YELLOW = MEETS MOST BUT NOT ALL CRITERIA	Y	7	13%
RED = MISSING OR DOES NOT MEET CRITERIA		45	83%
BLUE = EXCEEDS RATING CRITERIA		0	0
WHITE = NOT APPLICABLE	W	0	0
TOTALS		54	100%

The NSE Facility Plan, Procedures & Specifications Report was then developed based on the NSE Current State Assessment Report results.

In this report, GIT identified and developed an extensive array of:

- Facility focused Specifications and
- Emergency Response and Restoration Procedures

To guide the implementation of specifications and procedures, GIT developed a comprehensive implementation planning document that can also serve as a control and reporting mechanism. The Implementation Plan is supported by a set of DR standards, role definitions and templates that can be used to update, maintain and sustain the procedures and other plan documents.

To complete the DRP, GIT worked with the NSE staff to gather and document:

- Supplier Identification – 21 key suppliers of software, equipment and services in both Nigeria and the United States
- Development Impact Analysis – identified that the final DRP will enable NSE to maximize ROI on business processes
- Development Benefits Analysis – identified benefits and gains in Security, Reliability and Data Integrity
- Project Benefit Estimate – addressed potential improvements in Infrastructure Industry, Market-oriented reforms, Human Capacity building as well as Technology Transfer and Productivity.

GIT reviewed and determined that there will be no adverse impact on any regulations, laws, or that any institutional changes will be needed.

GIT determined with NSE's help that there is no potential adverse environmental impact from the DRP to local requirements and those of the World Bank.

GIT's success in completing this important project was facilitated by the responsiveness and support of the NSE team coordinated by Mr. Osita Ogbonnaya.

In order to prepare for efforts that will follow, GIT will continue to work with the NSE staff to ensure successful implementation, training and ongoing support of the NSE DRP.

INTRODUCTION

Background

The Nigerian Stock Exchange (NSE) was established in 1960 and had over 280 listed companies with a total market capitalization (at the end of 2005) of approximately $20 billion. All listings are included in the only index, the Nigerian Stock Exchange All Shares Index. The Nigerian Stock Exchange and its management team understand the importance of a reliable stock exchange and requested the U.S. Trade and Development Agency (USTDA) provide "Technical Assistance" to facilitate development of a disaster recovery plan (DRP).

The DRP will provide a mechanism for continuous trading and support of the NSE in case of failure of the main building or main equipment and ensure that the data stored and transferred on the NSE's hardware and communications infrastructure is fully recoverable and secure.

The Technical Assistance includes the review of existing IT systems and plans, existing hardware and communications infrastructure, and would develop a gap assessment, procedures and specifications, and an implementation plan for a disaster recovery facility. The Technical Assistance will also ensure that any recommended procurements can be integrated with existing hardware, communications infrastructure, applications, and databases.

Global Information Technology, Inc. (GIT) was awarded the contract to provide the services necessary to develop a DRP for the NSE on November 11, 2008. The project was funded in it's entirety by the United States Trade and Development Agency (USTDA) and to be staffed by GIT.

GIT received funding from the USTDA and began phase one of this project in February 2, 2009 and assembled a team on the ground in Lagos, Nigeria to begin the acquisition of the information and data necessary to begin to develop the plan.

An original project plan was distributed to the NSE team and a kick off meeting was conducted in March 3, 2009 (See Appendix 2: Letter of Invitation) where questionnaires were distributed (See Appendix 1: NSE Questionnaire) to the key members of the NSE team for the purpose of capturing the information GIT would require to build an effective DRP.

Objectives

The GIT team focused on completion of objectives outlined based on the NSE Annex I from USTDA:

- Phase I focused on NSE Annex I Tasks 1, 2, 3

- **The Current State Assessment Report was delivered to the NSE in January 2010**

- **Phase 2 focuses on the completion of NSE Annex I Tasks 4, 5, 6**
  - **The Facility Plan, Procedures & Specifications Report was delivered to the NSE in March 2010**
- **Phase 3 focuses on the completion of NSE DRP and includes Annex I Tasks 7-10**
  - **The Final DRP Report was delivered to the NSE in June 2010**

Scope of the Efforts

The overall scope of the work to be performed under this proposal is to:

- Produce the DRP Report for the NSE environments
- Define the time criteria for restoring the NSE's operating environment
- Document the provisions for recovery of mission critical IT processing capabilities and Applications within the time frames provided by the plan.

This project does not include funds to:

- Purchase any software tools or packages that may be recommended as a result of work on this project.
- Perform tests of the effectiveness of the disaster recovery procedures documented in the plan
- Conduct or support any new/modified Vendor Agreements
- Negotiate or support any new/modified internal Agreements
- Perform training on any selected and implemented tools.

GIT worked directly with the NSE liaison (Mr. Osita Ogbonnaya) to gather the necessary information to initiate, continue and complete this important project.

Key Stakeholders

The key individuals in preparation of the NSE BCP/DRP include:

NAME	ROLE	FUNCTION/RESPONSIBILITY
Professor Ndi Okereke Onyiuke	NSE Group MD, CEO	Project Support
Mr. Binos Yaroe	NSE GM Information Tech & Operations	Project Support
Mr. Taba Peterside	NSE GM Risk Management & Regulation	Project Support
Mr. Osita Ogbonnaya	NSE DGM Information Tech & Market Operations;	Liaison between the NSE and GIT project teams
Mr. Mike Ike	GIT Delivery Director	Facilitate project completion in Nigeria and US
Mr. Irv Brownstein	GIT Project Manager	Primary developer of the NSE DRP including the Current State Assessment Report and the Facility Plan, Procedures & Specifications Report
Mr. Dan Nebel	GIT Account Manager	Manage relationships with NSE and USTDA as well as facilitate project resource needs

Reader Guide and Document Summary Description

In order to aid the reader in finding key information, GIT prepared a summary of each component of the document. The descriptions below are provided in the general order that they appear in this document.

READ THIS SECTION...	IF YOU NEED TO KNOW ABOUT ...
INTRODUCTION	The key stakeholders; a description of each component of the document; and, a broad DR/BCP Glossary of terms Objectives - The GIT team focused on completion of objectives outlined based on the NSE Annex I from USTDA Background & Scope - The overall description of the Technical Support effort for NSE funded by the USTDA and performed by GIT.

READ THIS SECTION...	IF YOU NEED TO KNOW ABOUT ...
CURRENT STATE ASSESSMENT (CSA)	Highlight findings and gap assessments. Specifically GIT addressed five (5) broad areas: • Environment • Emergency Response Procedures • DR Plan Activation Procedures • NSE Administrative Procedures • DR Reports and Forms
GIT WORK APPROACH	How GIT developed the NSE DR Facility Plan, Procedures & Specifications Report incorporating the results and responses to the Phase I Current State Assessment report in six (6) broad steps focusing on the report preparation, development of an Implementation Plan as well as an array of procedures and checklists.
DR STRATEGIC NEEDS & SPECIFICATIONS	In this section, GIT outlines the needs, goals, security, and performance objectives for the future DR site. Specifically GIT addressed eight (8) broad areas: • Redundancy Needs • Service Level Agreement Expectations • Networking, Connectivity and Circuits • Power Consumption • Cooling Capabilities • Fire Protection • Data Replication • Site Plan
IMPLEMENTATION PLAN	GIT created a phased implementation plan for the DR facility highlighting seven (7) broad project Phases, related Tasks and associated Deliverables: • Complete DR Plan • NSE Data Completed • Supplier RFQ/RFP • Vendor(s) Selection • Build & Acquire

READ THIS SECTION...	IF YOU NEED TO KNOW ABOUT ...
	• Load & Test • Management Review The final implementation phase is followed by a recurring "Fire Drill" (or Test) phase/task to ensure that the DR Plan remains accurate, reflective and relevant to the NSE facilities.
NSE SUPPLIER & IMPACT RESULTS	This section describes the efforts going forward to establish the NSE DR Facility in terms of the: • Supplier Identification – 21 key suppliers of software, equipment and services in both Nigeria and the United States • Development Impact Analysis – identified that the final DRP will enable NSE to mximize ROI on business processes • Development Benefits Analysis – identified benefits and gains in Security, Reliability and Data Integrity • Project Benefit Estimate – addressed potential improvements in Infrastructure Industry, Market-oriented reforms, Human Capacity building as well as Technology Transfer and Productivity.
APPENDIX 1: NSE BCP/DRP PROJECT QUESTIONNAIRE	This Appendix provides the original questionnaire used to identify the current state of BCP/DRP data, procedures and standards. The information provided formed the basis for the Current State Assessment.
APPENDIX 2: LETTER OF INVITATION	This Appendix provides the format and content of a standard Letter of Invitation that must be properly executed to invite individuals to Nigeria.
APPENDIX 3: NSE NETWORK DIAGRAMS AND RESOURCES	This Appendix highlights the current NSE: • Hardware and Resources • Network • IT Infrastructure.
APPENDIX 4: NSE BCP/DRP DISASTER AND CONTINGENCY PLAN PROCESS	Business Continuation Planning Process charts provide guidance to NSE Business Continuation Planners. The process charts depict the array of phases, steps, and tasks associated with a comprehensive plan. The five broad phases includede are:

READ THIS SECTION...	IF YOU NEED TO KNOW ABOUT ...
	• Project Initiation; • Business Impact Analysis; • Strategy Selection; • Plan Preparation; and • Testing and Maintenance.
APPENDIX 5: DECISIONS RELATED TO FAILOVER VS. BACKUP	The Situation and Damage Assessment Team Leader selects appropriate personnel to travel to the damaged site to assess the damage. This Appendix describes the decision matrix the Team follows to determine actions related to the damaged facility.
APPENDIX 6: NSE EMERGENCY TEAM COMPOSITION	This Appendix highlights the critical formation of an Emergency Management Team and depicts the facilities needed.

APPENDIX 7: NSE RESOURCES	This Appendix describes the NSE resources in terms of:
	• Network
	  o Software
	  o Server hardware
	  o End User hardware
	  o Telecom
	• Interconnectivity
	• IT Infrastructure

APPENDIX 8: NSE IMPLEMENTATION WORK PLAN	The NSE Implementation work plan spans the seven broad Project Phases and over 40 Tasks in a table created for both planning and subsequent project control. The plan provides estimates for both effort and duration to complete the NSE DR facility. The format used facilitates focus on Deliverables and reporting progress to management
APPENDIX 9: NSE BCP STANDARDS	This Appendix describes twenty-four (24) standards grouped into five (5) key groups used by NSE to manage planning and execution of Business Continuity and Disaster

READ THIS SECTION...	IF YOU NEED TO KNOW ABOUT ...
	Recovery. The groups of standards are: • BC/DR Planning Related • BC/DR Recovery and Restoration Factors Related • BC/DR Testing Related • BC/DR Quality and Control Related • BC/DR Staff Related.
APPENDIX 10: NSE BCP PLAN, EMERGENCY ACTIONS & PROCEDURES	This Appendix contains extensive information and detailed procedures for Emergency Response, Recovery, and Restoration operations for NSE departments in the event of a disruption including: • Procedures that allow NSE departments to respond appropriately to a business disruption • The teams that complete the specific activities necessary for emergency response and recovery • The critical business functions that need to continue after a disaster • The logistics of recovering critical business functions • The procedures for releases of information to employees and the general public • Ensure the safety of employees and visitors of NSE departments
APPENDIX 11: NSE DR RESPONSE & RECOVERY CHECKLIST	This Appendix provides a series of DR Checklists and Templates addressing: • Emergency Contact • Emergency Procedures & Instructions for Fire • DR Restoration Actions
APPENDIX 12: SAMPLE – NSE DR PROCEDURE GUIDE	This Appendix provides a sample DR guide for NSE that includes: ➢ Emergency Levels ➢ Emergency Response Team Actions & Instructions; ➢ Hazards and Threats with profiles for each and ➢ First Response Steps to Take; ➢ Configuration setup for the Alternate Site; Recovery Priorities; and,

READ THIS SECTION...	IF YOU NEED TO KNOW ABOUT ...
	▪ Checklist of Actions to take
APPENDIX 13: SAMPLE – MUMBAI DRP	This Appendix provides Sample DRP of the National Stock Exchange of Mumbai. The DRP includes: ▪ Background and structure of the Exchange ▪ Key IT Infrastructure at the Primary Site ▪ Detailed Systems Architecture ▪ Project Design – BCP essentials & Description of key activities; Timeframes & Implementing Agencies ▪ Change Management Strategy ▪ Deployment & Business Models ▪ Standard Operating Procedures ▪ Operational Best Practices for DR & BCP
APPENDIX 14: NSE SUPPLIER AND IMPACT QUESTIONNAIRE & RESPONSE	This Appendix provides the questionnaire and results used to build the Supplier and Impact information. This questionnaire addresses: • Supplier Identification • Development Impact Analysis • Development Benefits Analysis • Project Benefit Estimate
APPENDIX 15: NSE PROPOSED ORGANIZATION PLAN & CHARTS	This Appendix highlights the proposed NSE organization structure including: • Office of the Director General • Quotation/Listing Division • Operations Division • Bonds/Derivatives Markets Division • Support Services Division
APPENDIX 16: NSE BCP/DRP PROJECT QUESTIONNAIRE RESPONSE	This Appendix provides the responses from the NSE that formed the basis for the Current State Assessment Gap Analysis.
APPENDIX 17: GIT NSE DRP PROPOSAL FOR TECHNICAL	This Appendix incorporates the proposal developed and submitted by GIT to provide Technical Assistance for

READ THIS SECTION...	IF YOU NEED TO KNOW ABOUT ...
ASSISTANCE	USTDA to the NSE.
APPENDIX 18: NSE ORIGINAL ANALYSIS	This Appendix incorporates the original study that identified the need for Technical assistance to the NSE.

DR BCP Acronyms and Glossary of Terms

A number of key Terms that are used throughout the process, procedure, checklists and documents are defined below for all of the components of the NSE DRP/BCP.

TERM	DEFINITION
ALTERNATE SITE	A location, other than the normal facility, used to process data and/or conduct critical business functions in the event of a disaster.
APPLICATION RECOVERY	The component of disaster recovery and testing which deals specifically with the restoration of business system software and data, after the processing platform has been restored or replaced
ASSUMPTIONS	Basic understandings about unknown disaster situations that the business continuation plan and plan testing are based on.
BC	Business Continuation
BCP (BUSINESS CONTINUATION PLANNING)	An all encompassing "umbrella" term covering both disaster recovery planning and business resumption planning.
BIA (BUSINESS IMPACT ANALYSIS)	The process of identifying the business processes critical to the profitability and survival of the organization's operations. The process can be broken down into four steps: 1. Determining the scope of the analysis; 2. Gathering the initial information about business unit functions, support systems, and applications 3. Conducting interviews to verify the completeness and accuracy of information gathered 4. Analyzing the information to determine priorities, assigning recovery time objective (RTOs), and presenting these results to the appropriate management level for review and validation.
BUSINESS FUNCTION	A logical group of business processes which consist of procedures and/or tasks having the end goal of meeting a business need.
BUSINESS GROUP	A high level entity that is comprised of various Business Units. Examples of Business Groups are: TPG Insurance, Diversified Group, etc.
BUSINESS PROCESS	A set of tasks and/or procedures which accept a specific work

TERM	DEFINITION
	input and generate a specific work output.
BUSINESS UNIT	A department or legal entity in the NSE designated to perform a line or staff function as designated by a Business Group or Corporate Functional Area. A business unit may also be a corporate function such as Legal or Human Resources.
COLD-SITE	A cold-site (also referred to as a shell site) is a site where the computer environment is maintained without any equipment; it is a computer room without the computer. Cold-sites are commercially available or may be maintained by the organization itself. The major task involved in the use of a cold-site is the location, purchase, transportation, and installation of replacement hardware. Also involved is the installation of electrical, communications, and environmental related work. Any services required to prepare a cold-site (i.e., electrical contractors, network professionals) should be pre-arranged and documented in the BCP.
CRITICAL BUSINESS FUNCTION	A logical group of NSE business processes which consist of procedures and/or tasks having the end goal of meeting a business need *and* that would have a significant impact on the organization if not performed. The impact is usually measured quantitatively (cost per hour/day/week that not processing that function would cost the business unit) and/or qualitatively (the business reason why that function is necessary to the survival of the organization) as part of the business impact analysis.
DAG	Delegation of Authority Guidelines
DAMAGE ASSESSMENT	The process of assessing damage, following a disaster, to computer hardware, vital records, office facilities, etc. and determining what can be salvaged or restored and what must be replaced
DEPARTMENT	A distinct, usually specialized division of a business unit within NSE
EBCO	Enterprise Business Continuation Office
EMT	Emergency Management Team
EOC	Emergency Operations Center
FULL BUSINESS TEST	This test requires the simulated recovery of critical business functions across a business unit – it is the closest exercise to an actual disaster. Although a full operations test requires weeks of

TERM	DEFINITION
	planning and considerable coordination of personnel and resources, the exercise provides a business unit with a level of confidence about their ability to recover in an actual event.
GAP ANALYSIS ASSESSMENT	In information technology a gap analysis is an assessment tool to help identify the differences between "where we are and where we want to be." A gap analysis helps bridge that space by highlighting which requirements are being met and which are not. The gap analysis provides a foundation for measuring the investment of time, money and human resources that's required to achieve a particular outcome.
HOT-SITE	A hot-site is a computer center in a ready state in case of disaster. Hot-sites are commercially available. Cost is dependent on the amount of hardware, floor space required, communications requirements, and services supplied but is generally high, ranging from tens of thousands to hundreds of thousands of dollars per year. Many hot-sites also have initial subscription fees and a disaster declaration charge which prevents the customer from using the facilities for extra processing power during normal operations. A specified set of testing is normally allowed and a charge levied for any extra testing.
INTERDEPENDENCY	The internal and external service provider(s) and source(s) of work received from other internal and external business units that the business unit relies on for processing their business functions.
IRAC	The Incident Response and Alert Center, is the single point of contact for reporting actual and potential business disruptions. IRAC will mobilize the necessary internal resources based on the nature of the event being reported and the business unit(s) affected. Generally, these contacts include: Corporate Technology Services, Corporate Real Estate, Management Internal Control, the Chief Information Officer, and the affected business unit's group executive. Optional contacts include: Corporate Compliance, Counsel, Investigations, Security, Risk Management, General Audit and the Operations and Systems Executive.
LAN	Local Area Network
MIC	Management Internal Control
RECIPROCAL	An agreement with a compatible organizational unit that may have

TERM	DEFINITION
AGREEMENT	excess capacity. Both organizational units must have the need for a backup site and be able to give up space and/or processing time in the event of a disaster occurring at the other organizational unit.
RECORDS MANAGEMENT	The NSE area charge with actively maintaining the NSE vital records
RECOVERY POINT OBJECTIVE (RPO)	A 'RPO' is the point in time that a Business function must be able to recover all of its critical data from the last backup cycle or off site retrieval
RECOVERY TIME OBJECTIVE (RTO)	A 'RTO' is the time frame by which the organization's critical business functions must be recovered. In other words, it is the maximum amount of time that the function can be suspended before causing a severe impact to the unit's goals and responsibilities.
SCOPE	Predefined areas of operation for which a business continuation plan is developed
SERVICE LEVEL AGREEMENT (SLA)	A service level agreement (SLA) is a negotiated agreement between two parties where one is the customer and the other is the service provider. This can be a legally binding formal or informal "contract" with an internal department. The SLA typically records a common understanding about services, priorities, responsibilities, guarantees, and warranties.
UPS (UNINTERRUPTIBLE POWER SUPPLY)	Backup power used when the electrical power fails or drops to an unacceptable voltage level. Small UPS systems provide battery power for a few minutes; enough to power down the computer in an orderly manner. Sophisticated systems are tied to electrical generators that can provide power for days.
VITAL RECORDS	Those records necessary to continue business operations after a disaster
WARM-SITE	An alternate processing site which is only partially equipped (as compared to a hot-site which is fully equipped).

GIT WORK APPROACH

Assessment and Evaluation

GIT utilized a set of proprietary templates to gather and document the critical DRP information for the current phase of the project.

To accomplish this component of the Technical Assistance for NSE, GIT:

- Reviewed existing IT systems and plans, existing hardware and communications infrastructure (See Appendix 3: NSE Network Diagrams and Resources, Appendix 15: NSE Proposed Organization Plan & Charts), and
- Reviewed the data gathered from the Questionnaire (See Appendix 16: NSE BCP/DRP Project Questionnaire Response)
- Compared the information gathered to industry-based Disaster Recovery Planning Best Practices
- Evaluated, rated, scored and documented a resulting Gap Analysis as a critical component of the "NSE DR Current State Assessment" to be delivered to NSE.

GIT then:

- Utilized the Gap Analysis and DR Assessment along with the DR Best Practices and its extensive experience to develop and document the critical procedures, forms and reports that will be integrated into an overall NSE DR Facility Development and Implementation Plan.
- Ensured that any recommended procurements can be integrated with existing hardware, communications infrastructure, applications, and databases.

Over the course of the overall project, GIT specifically will:

1. Complete DR Data Gathering & Current State Assessment
2. Document Critical Procedures
    - Emergency Response Procedures
    - Plan Activation Procedures

- Administrative Procedures

3. Document Key DR Reports and Key DR Forms
4. Complete Final Delivery & Reporting

In each phase of the NSE DRP Project, GIT will complete one or more key Tasks as outlined in the original proposal (See Appendix 17: NSE DRP GIT Proposal).

Note: the GIT Proposal is based on recommendations made to the NSE that are documented in Appendix 18: NSE Original Analysis.

DR Data Gathering & Current State Assessment

GIT completed this stage of the project in three broad tasks:

- Identified key Areas/individuals
- Distributed/Conducted Data Gathering Template(s)
- Completed Gap Analysis & DR Assessment

The Questionnaire Guide was used to identify and gather input into the NSE Disaster Recovery Planning & Business Continuity Planning project.

The Questionnaire is made up of a number of questions in five (5) broad areas pertaining to information that GIT has found to be important to the successful development and implementation of the NSE DRP. These areas include:

- Current NSE Environment
- NSE Emergency Response Procedures
- NSE DR Plan Activation Procedures
- NSE Administrative Procedures
- NSE DR Reports & Forms

A set of General Instructions (see below) were used to guide completion:

> **Enter** the information that "best" represents your specific understanding about the Disaster Recovery and Business Continuation needs for NSE. Add extra information wherever necessary – attach any information requested.
>
> **CIRCLE your answer to each question.** Please do not guess: if you don't know the answer, don't respond to the question. Keep in mind that you can identify that you "Don't Know" (DK) for any question area(s) that do not apply to your job, or where you have no direct information.
>
> **Please enter as much clarifying information as you can**.
>
> Note: All of the information entered this questionnaire will be held in strict confidence.

CSA Data Analysis and Scoring

Each response provided by the NSE on the Questionnaire and related information was compared to and evaluated against the GIT BCP/DR Best Practices the Rating System shown below:

LEGEND

GREEN = MEETS ALL CRITERIA	
YELLOW = MEETS MOST BUT NOT ALL CRITERIA	Y
RED = MISSING OR DOES NOT MEET CRITERIA	
BLUE = EXCEEDS RATING CRITERIA	
WHITE = NOT APPLICABLE	W

As appropriate, all relevant support information was also captured and documented in the Assessment in order to facilitate analysis and preparation of the various DRP Procedures.

DR Facility Plan, Procedures & Specifications Report Project Steps

GIT developed the NSE DR Facility Plan, Procedures & Specifications Report incorporating the results and responses to the Phase I Current State Assessment report by completing the following six (6) broad steps:

1. Completed Task#4 - DR Strategic Needs & System Requirements
2. Completed Task#5 - DR System Specification
3. Completed Task#6 - DR Implementation Plan
4. Prepare Report
5. Conduct Internal & NSE reviews
6. Prepare Final Report for NSE Approval – based on internal review feedback

Facility & Specification Report Preparation

GIT utilized a set of proprietary templates to gather and document the critical DRP information for the current phase of the project.

To accomplish this component of the Technical Assistance for NSE, GIT:

- Reviewed the Current State Assessment Report
- Focused on the expected content outlined in NSE Annex I - The NSE DRP Facility Work Plan is based on the content and focus of each Component of NSE Annex I Tasks 4, 5, and 6
- Researched content specification - Reference & Support materials was incorporated as identified, defined and/or developed.
- Combined the results from NSE Annex I tasks 4 and Task 5 into a single section focused on specifications

The data from completing NSE Annex I Tasks 4, 5, and 6 was incorporated into a single overall document similar to the Current State Assessment Report: titled "The NSE DRP Facility Plan, Procedures & Specifications Report". The NSE DRP Facility Plan, Procedures & Specifications Report had an overall Table of Contents with all associated attachments in the Appendix.

NOTE: See the separate section of DR System Specifications in this report.

NSE CURRENT STATE ASSESSMENT (CSA)

Current NSE Environment - Assessment

Each element of the Current NSE Environment was evaluated and Rated using the Rating Criteria identified at the end of this section.

[illegible]	[illegible]	[illegible]
Is there an NSE Disaster Recovery (DR) POLICY Statement?	[illegible]	➢ **No, per Osita**
Is there a current DR PLAN?	[illegible]	➢ **No, per Osita**
Is there a complete and up to date Emergency Contact List?	[illegible]	➢ **No, per Osita**
Is there a complete and up to date APPROVAL List?	[illegible]	➢ **Professor Ndi Okereke Onyiuke, Group MD, CEO** ➢ **Mr. Binos Yaroe, GM Information Tech & Operations** ➢ **Mr. Taba Peterside, GM Risk Management & Regulation** ➢ **Mr. Osita Ogbonnaya, DGM Information Tech & Market Operations**
Is there a FAIL-OVER SITE?	[illegible]	➢ **No, per Osita**
➢ **Is there a current FAIL-OVER SITE agreement?**	[illegible]	➢ **No, per Osita**
➢ **Has the FAIL-OVER SITE been tested in a formal fire-drill?**	[illegible]	➢ **No, per Osita** ➢ **No results**
Identify current NSE processing VOLUMES? ➢ For each Transaction type – identify the Volume, Period, Peak period volumes	**Y**	➢ **Somewhat, per Osita** o Identified as available o No data supplied

[illegible]	[illegible]	[illegible]
▪ Identify the general volume history over the past 24 months (or attach separate report covering the same data).		
Identify Failure history over the past 18 months?	[redacted]	▪ **No, per Osita** o "**No plan in place to document this information**"
Identify KEY CONTACT INFORMATION related to each critical business function?	[redacted]	▪ **No, per Osita** o "**Not clearly defined for now**"
Identify Software used to support NSE?	[redacted]	▪ **No, per Osita** o Requested List or Report
Identify Current NETWORK for both data and telecommunications?	[redacted]	▪ **No, per Osita** o Provide one or more systems architecture chart(s) that highlights each element of the o IT Infrastructure depicting each device type o Telecommunications protocols
Identify BUSINESS UNIT INVOLVEMENT with the NSE DR?	[redacted]	▪ **No, per Osita** o No people are involved from the business units in BCP planning o No one is accountable for plan content development and approval o No one participates in testing exercises
Identify NSE SECURITY related to the NSE DR?	**Y**	▪ **Somewhat per Osita** o "**Although fulltime security personnel are in place, there are no predefined roles during an outage**".
Identify NSE EXECUTIVE SPONSORSHIP?	[redacted]	▪ **No, per Osita** o No one is responsible for Business Continuity Planning o Organizational structure – under development o No steering committee

[illegible]	[illegible]	[illegible]
		○ No frequency to review plan readiness and issues ○ No board of directors for BCP review
Perform NSE RISK ASSESSMENT?		▪ **No, per Osita** ○ No one performs routine facility risk assessments ○ No one meets with local fire, police, and Hazardous Material teams to ensure assumptions in plan are within their guidance ○ No one has identified internal and external threats ○ There are no controls in place to monitor Security, Life Safety, and Communication to Personnel ○ No one has developed risk exposures and financial cost analysis

LEGEND

GREEN = MEETS ALL CRITERIA	
YELLOW = MEETS MOST BUT NOT ALL CRITERIA	Y
RED = MISSING OR DOES NOT MEET CRITERIA	
BLUE = EXCEEDS RATING CRITERIA	
WHITE = NOT APPLICABLE	W

NSE EMERGENCY RESPONSE PROCEDURES - Assessment

Emergency response ensures that all parties act to quickly determine the emergency and take appropriate action. GIT will complete this stage of the project in three tasks:

- Emergency Evacuation Procedures
- Emergency Phone Numbers
- Emergency Notification Procedures.

A business disruption has three distinct phases: Emergency, Recovery, and Restoration. The emergency operations center (EOC) is the focal point of communication and coordination for resources during a business disruption.

Each element of the NSE Emergency Response Procedures was rated using the Rating Criteria identified at the end of this section.

[redacted]	[redacted]	[redacted]
Is there an EMERGENCY MANAGEMENT TEAM?	[redacted]	▪ **No, per Osita**
Is there an EMERGENCY OPERATION CENTER?	[redacted]	▪ **No, per Osita**
Are there documented EMERGENCY PROCEDURES?	[redacted]	▪ **No, per Osita** ○ There is no chart that outlines the procedure steps that address notification and mobilization ○ There is no emergency procedure available yet to identify the procedures that indicate what steps are followed AND who (Name & Title) is responsible for the specific actions.
Identify the current NSE EMERGENCY CONTACT LIST?	[redacted]	▪ **No, per Osita** ○ " **Not available**"

LEGEND

GREEN = MEETS ALL CRITERIA	
YELLOW = MEETS MOST BUT NOT ALL CRITERIA	Y
RED = MISSING OR DOES NOT MEET CRITERIA	
BLUE = EXCEEDS RATING CRITERIA	
WHITE = NOT APPLICABLE	W

NSE DR PLAN ACTIVATION PROCEDURES - Assessment

Plan activation ensures that all parties and all materials are coordinated for the DR Facility. GIT will complete this stage of the project in ten (10) tasks:

- Activate Incident Management Team
- Activate Emergency Operations Center
- Emergency Declaration Procedures
- Relocate Operations Procedures
- Situation & Damage Assessment Procedures
- Communications
- Offsite Storage
- Purchasing procedures
- Recovery Site Generator, Electrical & Security plan Procedures
- Reconstruction Procedures

Each element of the NSE DR Plan Activation Procedures was rated using the Rating Criteria identified at the end of this section.

[illegible]	[illegible]	[illegible]
Identify Mission CRITICAL BUSINESS FUNCTIONS AND PROCESSES?	[redacted]	▪ **No, per Osita** o For each critical function service, product and/or system there is no defined the time-frame (Notification and Recovery) that it must be fully operational
Is there a RECOVERY STRATEGIES Associated With Each Business Segment?	[redacted]	▪ **No, per Osita** o For Transfer of Work o For in-house Recovery o For work from Home
Is there a Defined RECOVERY ORGANIZATION?	[redacted]	▪ **No, per Osita** o Name and Function
Are there defined ROLES AND RESPONSIBILITIES?	[redacted]	▪ **No, per Osita** o Function, Role and Responsibility
Are there defined Procedure Steps for the EMERGENCY	[redacted]	▪ **No, per Osita** o Step, Name and Procedure

[illegible]	[illegible]	[illegible]
PHASE?		
Are there defined Procedure Steps for the RECOVERY PHASE?		▪ **No, per Osita** o Step, Name and Procedure
Are there defined Procedure Steps for the RESTORATION PHASE?		▪ **No, per Osita** o Step, Name and Procedure
Are there defined RESOURCES - Software, Hardware and Supplies associated with the procedures?		▪ **No, per Osita** o References to space, specific supplies, software names and versions, hardware devices

LEGEND

GREEN = MEETS ALL CRITERIA	
YELLOW = MEETS MOST BUT NOT ALL CRITERIA	Y
RED = MISSING OR DOES NOT MEET CRITERIA	
BLUE = EXCEEDS RATING CRITERIA	
WHITE = NOT APPLICABLE	W

NSE ADMINISTRATIVE PROCEDURES - Assessment

The administrative responsibilities summarize NSE policy. These responsibilities and procedural guidelines must be applied throughout the initial response and any subsequent business recovery activities.

- Enforce NSE Policies
- Monitor & Report Recovery process
- Maintain Recovery Related Record Keeping
- Define Testing & Maintenance Functions

Each element of the NSE Administrative Procedures was rated using the Rating Criteria identified at the end of this section.

[illegible]	[illegible]	[illegible]
Is there a Defined MAINTENANCE SCHEDULE?	Y	▪ **Somewhat, Not comprehensive, per Osita** ○ "**Only for some IT & Building equipment**"
Are there defined and documented events that trigger a MAINTENANCE REVIEW?		▪ **No, per Osita** ○ "**Anything because of structured approach to problem resolution**" ○ No defined Situation and Actions Taken
Are DISASTER RECOVERY PLAN UPDATES Made On A Scheduled Basis?		▪ **No, per Osita** ○ "**No plan yet**" ○ No distribution
Are there DIRECTIONS to Emergency Operations Centers?		▪ **No, per Osita** ○ Function, Role and Responsibility
How are Policies ENFORCED?		▪ **No, per Osita** ○ "**No policies in place yet**"
How is Record Keeping MAINTAINED?	Y	▪ **Somewhat, per Osita** ○ "**Manually on files and cabinets for now**"
Is there a DAMAGE ASSESSMENT CHECKLIST?		▪ **No, per Osita** ○ "**None yet**"
Is there a FACILITIES EMERGENCY		▪ **No, per Osita** ○ "**None yet**"

[illegible]	[illegible]	[illegible]
PROCEDURES?		
Is there an ORGANIZATION CHART with a Master Employee Listing?	**Y**	▪ **Somewhat, per Osita** o See Appendix 15: NSE Organization Chart – dated April, 2006 o "**But a new one is in development**"
How frequently is the call tree updated?		▪ **No, per Osita** o "**Not yet available**"
Is there a RECOVERY STATUS REPORT?		▪ **No, per Osita**
Is there an APPROVED PRESS RELEASE?		▪ **No, per Osita**
Is there a MAINTENANCE LOG?	**Y**	▪ **Somewhat Per Osita** o "**Only for some IT equipments** o "**Backup generators and office equipment**" o But formal LOF Book in place o No material available
Describe the NSE Profile		▪ **Yes, Responses per Osita** o How long has NSE been in business? **49 Years** o How many locations does NSE have? **20+ Branches, 1 HQ** o What is the number of people by location? **TBD** o How many people are within NSE overall? **Approx 300** o Please define the organizational structural by business unit? **Still in Development** o What percent of the NSE budget is dedicated towards BCP? **None** o Does NSE currently have a BCP Steering Committee? **No** o Who are NSE's primary client(s)? Where are they located? **Brokers, Listed COYS, Government Regulators, Banks, Registrars, Publics, Foreign Investors, Globally Located.**
How is Client		▪ **No, per Osita**

TOPIC	RATING	COMMENTS/REFERENCE
COMMUNICATION handled about NSE "Disasters"?	[redacted]	○ What is communicated to your clients concerning BCP? **"Nothing"** ○ Do you track what was said and to whom? **"No"** ○ Do you receive inquiries from clients? "**Sometimes"** ○ Do clients ask for onsite visits? **"No"** ○ Do you have a centralized repository for issue management? **"Various Units"** ○ Who is overseeing closure of critical issues? **"Various Units"** ○ Do you utilize any tools for mass communication? Do you utilize your website? **No Response** ○ How do you to communicate to personnel during a situation? **"By Phone"** ○ How frequently do you communicate plans status, evacuation plans, and life safety preparedness to your personnel? **"Rarely"** ○ Do you have a plan to communicate to external vendors and clients? Have you tested this? When and What was the result? "**None yet"**
What are the NSE DR PROGRAM CONTROLS?		▪ **No, per Osita** ○ How do you monitor your plan readiness**? "N/A"** ○ What metrics do you use for testing of plan content? "**None Yet"** ○ What percent of people participate in business unit testing? **"None"** ○ Do you review your program with Legal/Compliance teams? "**N/A"**
***Identify* NSE DR PROGRAM MATURITY?**		▪ **No, per Osita** ○ Have you instituted a firm-wide plan for business continuity? "**No"** ○ Are key members of your businesses involved? **"None Yet"** ○ What percent of BCP activities are

		completed with Information Technology? "**Data Backup Only**"
Identify NSE LIFE SAFETY *related to the* NSE DR?		➢ **No, per Osita** o Do you have first aid responders within your buildings? **"No"** o What is the frequency of their training? "**None**" o Do you personnel know who they are and how to engage with them? "**No**" o Do you they have role within the Incident Management Plan? "**None Yet**"
Identify NSE INCIDENT MANAGEMENT PROGRAM related to the NSE DR?		➢ **No, per Osita** o Do you include life safety, security, business units, and IT in your incident management program? **No Response** o Do you have a location near the building for people to gather in a evacuation? **"No"** o Do you have a mechanism to verify all people have safely left the building? "**No**" o Do you have a Incident Manager for each site in your organization? "**No**" o Do you have a checklist for that person to execute and provide status? **"None"** o Have roles and responsibilities been clearly assigned for during the event? **"No"**
Identify NSE INDUSTRY TESTING related to the NSE DR?		➢ **No, per Osita** o Do you participate in industry testing? "**No**" o Do you test with your critical vendors? "**Yet to Start**" o What level of participation is required? "**Not known yet**" o How frequently do you test? **"No Testing Carried Out Yet"**

TOPIC	RATING	COMMENTS/RESPONSE
Identify NSE BACKUP SITE INVOCATION PLANS related to the NSE DR?	**Y**	▪ **Somewhat, per Osita** ○ Do you have steps to activate your backup site? "**Yes But Limited in Scope**" ○ Do they include communication, transportation, and logistics? "**Yes**" ○ Do you have decision points contained in the plan? "**No Documented Plan Yet**"

LEGEND

GREEN = MEETS ALL CRITERIA	
YELLOW = MEETS MOST BUT NOT ALL CRITERIA	Y
RED = MISSING OR DOES NOT MEET CRITERIA	
BLUE = EXCEEDS RATING CRITERIA	
WHITE = NOT APPLICABLE	W

NSE DR REPORTS AND FORMS - Assessment

Reports are a critical mechanism for communication throughout and after the Disaster/Recovery period. These include:

- Business Unit Key Contacts
- Summary of Critical Applications, Servers & Recovery Time Objectives (RTOs)
- Vendors & Suppliers
- Summary of Desktop & Workspace Requirements
- Other Equipment
- Critical Telephone Numbers Report

Forms are a critical support provided to all Recovery Teams for use throughout and after the Disaster/Recovery period. These include:

- Recovery Activities Log
- Critical Files & In-Progress Assessment
- Critical Equipment & Assessment
- Personnel Locations Control Form
- Time Sheet tracking
- Telephone Log
- Damage Control Status
- Bomb Threat Response
- Injury Status Reporting
- Receiving Room Sign-In

Each element of the NSE DR Reports and Forms was rated using the Rating Criteria identified at the end of this section.

[illegible]	[illegible]	[illegible]
Are key DR REPORTS used by NSE?	[redacted]	➢ **No, per Osita** ○ Business Unit Key Contacts. **"No"** ○ Summary of Critical Applications, Servers & Recovery Time Objectives (RTOs) **"No"** ○ Vendors & Suppliers **"N/A"**

[illegible]	[illegible]	[illegible]
		○ Summary of Desktop & Workspace Requirements **"N/A"** ○ Other Equipment **"N/A"** ○ Critical Telephone Numbers Report **"N/A"**
Are key DR FORMS used by NSE?		▪ **All Not Applicable, per Osita** ○ Recovery Activities Log ○ Critical Files & In-Progress Assessment ○ Critical Equipment & Assessment ○ Personnel Locations Control Form ○ Time Sheet tracking ○ Telephone Log ○ Damage Control Status ○ Bomb Threat Response ○ Injury Status Reporting ○ Receiving Room Sign-In
Identify NSE DATA STORAGE related to NSE DR Data?		▪ **No, per Osita** ○ Do you currently backup your servers? **"Yes but highly inadequate"** ○ Do you utilize a third party for this service? **"No"** ○ Have you reviewed their BCP plan? **"N/A"** ○ Did this meet or exceed your requirements for service? **"N/A"** ○ What medium is utilized for this function? **"N/A"** ○ How frequently is this completed? **"N/A"** ○ Have you successfully tested recovering this data at an alternative location? **"N/A"** ○ Did this test meet or exceed your recovery objectives? **"N/A"**
Identify NSE VITAL RECORDS related to NSE DR?		▪ **No, per Osita** ○ Have you inventoried your critical records? "**Not Quite**" ○ Have you secured offsite storage? **"No"**

[illegible]	[illegible]	[illegible]
		○ What percent of records are remaining onsite? **"N/A"** ○ How frequently do you send offsite? **"N/A"** ○ Have you visited the site as part of due diligence? **"N/A"** ○ Have you tested that you could retrieve critical records in the time stated in service level agreement? **"N/A"**

LEGEND

GREEN = MEETS ALL CRITERIA	
YELLOW = MEETS MOST BUT NOT ALL CRITERIA	Y
RED = MISSING OR DOES NOT MEET CRITERIA	
BLUE = EXCEEDS RATING CRITERIA	
WHITE = NOT APPLICABLE	W

DR STRATEGIC NEEDS & SYSTEM SPECIFICATIONS

In this section, GIT outlines the needs, goals, security, and performance objectives for the future DR site. Specifically GIT addressed eight (8) broad areas:

- Redundancy Needs
- Service Level Agreement Expectations
- Networking, Connectivity and Circuits
- Power Consumption
- Cooling Capabilities
- Fire Protection
- Data Replication
- Site Plan

The objective of this effort was to prepare and submit detailed documentation of the work performed, including the general and technical DR specifications.

Hardware & Software Specifications

The GIT focus was to provide sufficient details of specifications of hardware, software, security equipment, network and communications infrastructure equipment, applications, and any other equipment from Task 4.

Note: These specifications (See Appendix 7 Current NSE Resources) were prepared to a level of detail that is not "vendor-specific".

DR Facility Specifications

The GIT focus was to establish procedures and pecifications that will be used in the bidding/procurement process and shall therefore be as accurate as possible given the requirements, dependencies, and assumptions of the DR project.

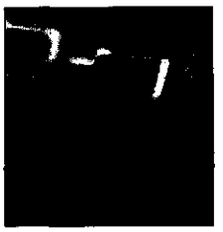
Note: These specifications were prepared to a level of detail that is not "vendor-specific".

Documented General & Technical Specifications.

The GIT focus was to prepare overall recommendations to support vendor bids and plans for the construction of the DR facility or modification of an existing facility as well as integration with existing systems, the equipment needs identified in the DR Strategic Plan, and system security

Note: These specifications were prepared to a level of detail that is not "vendor-specific".

Redundancy Needs



GIT evaluated the technical, business, and logistics information for preparedness in case of fire.

- The main threat to the operations of the Nigerian capital market at this time is the threat of fire that is electrical or accidentally started.

- The office spaces are overcrowded and outside help cannot be relied upon due to the Annex 1-2 location of the building, the height of the building and the gridlock traffic pattern in the district making it hard to access.

- Other factors weighing negatively are the:
  - Exit unfriendly building design
  - Lack of running water in the building or the vicinity thereof, as well as the
  - Lack of experience in extinguishing high-rise building fires by the Lagos Fire Department.

In order to meet this need, GIT drafted disaster and contingency plans allowing for system redundancy and back-up in the event of a building loss (See Appendix 10).

GIT also recommends that NSE employ a number of preventative measures to minimize the liklihood of building loss or to avoid emergencies or lessen the impact of a particular event as well as increase the likelihood of successfully recovering from a disaster. Note that all of the items on the checklist may not apply to each business unit. Additional preventive measures may need to be considered by the business unit.

- ☑ Investigate power continuation alternatives such as uninterruptible power supplies (UPS), generators, power conditioners, voltage regulators, and surge suppressors.

- ☑ Invest in first-aid/medical kits to help ensure personnel safety. Kits may include gauze, pads, splints, tapes, ointments, and bandages. Encourage CPR and first aid training.

- ☑ Store paper records in acid-free cardboard cartons.

- ☑ Safeguard electronic data with appropriate backup strategies such as tape backup, RAID technology, and electronic vaulting.

- ☑ Store data in different geographic locations.

- ☑ Investigate fire-proof and water-proof filing cabinets for on-site storage of vital records and data.
- ☑ Develop and document executive succession plans and procedures.
- ☑ Promote computer security awareness within your organization.
- ☑ Investigate the use of power failure transfer units to ensure access to telephone/fax lines in the event of a telecommunications disruption. Investigate emergency or alternate route services and alternate long-distance carriers for voice continuation.
- ☑ Educate your workforce in business continuation related issues via conferences, videos, and training manuals.
- ☑ Utilize equipment securing and restraining devices in areas affected by earthquakes. Water-proof, flame retardant covers are available to protect sensitive electronic equipment.
- ☑ Work with Corporate Real Estate to assess facility related threats.
- ☑ Test data and application restoration abilities regularly. Maintain frequent backups off-site.
- ☑ Keep computer equipment in low-traffic environments that are dry, clean, and dust-free.
- ☑ Never attempt to operate computer equipment that has been damaged due to heat, moisture, or soot until clearance is received from technology support services.
- ☑ Restrict access to facilities and computer rooms.
- ☑ **Explore advance arrangements for recovery services (hardware restoration, transportation requirements, document restoration services, etc.).**

The secondary objective of the Redundancy is to provide a mechanism for continuous trading and support of the exchange in case of failure of the main building or main equipment.

- Business continuation of processes and services is critical for an expanding exchange where volume transactions are doubling each year and capitalization is growing at 30% annually.

GIT defined the <u>decisions related to failover vs. backup</u> and the impact that will result from each chosen method (<u>See Appendix 5</u>).

Service Level Agreement (SLA) Expectations.

GIT researched and evaluated the criteria for the operations and data to be fully recovered in real-time status.

To achieve this, GIT recommends that there must be:

- **Real-time replication between the NSE independent production and DR data centers,**
  - GIT recommends two physical data centers, each running independently with only network failover.
  - When data is sent, it must be sent independently to both centers at the same time.
  - The only common element is connectivity to the corporate backbone network.
- **Automatic failover of:**
  - All systems to the DR facility.
  - All NSE databases and servers.
  - CSCS off-site backup server and depository.
- **Full availability of databases**
  - All data and history must be available.
  - The percentage of NSE operations that must be continued in case of disaster is 30%.
- **Performance of the DR facility and equipment**
  - Must match 100%. to the performance of the Production environment
  - Uptime of 99% and availability of the DR facility in case of failover
  - Establishment of maintenance windows for emergency support.
  - A Support team of technicians in order to provide tech support and guidance with the applications and servers in the DR facility.
  - GIT has defined the composition of the team and their general qualifications (See Appendix 6).
- **Business and Operational applications**
  - Trading, settlement and surveillance and the need for uninterrupted service.
  - All current Operational NSE and CSCS applications.

- Other applications and the target needs for service and update such as the Sybase Fusion server for online trading and account management and investor information.

- **Workstations and Printers**
  - GIT recommends a minimum of 20 workstations preloaded with trading software must be located in the new DR facility so trading in Lagos can continue.
  - GIT recommends a minimum of 14. Printers must be installed at the DR facility.

Note: Additional Resource Requirements and Needs as well as Actions & Related Procedures are identified and described in Appendix 7, 10 and 11.

Networking, Connectivity and Circuits.

GIT researched and evaluated the criteria for the network support needed for NSE operations and data to be fully recovered in real-time status.

To acieve this, GIT recommends that:

- **The DR data center must be supported by a network that is designed with the network connectivity and security equipment for successful, reliable operation after a DR Failover.**
  - The network must allow the market operators such as investors, brokers, settlement banks, the Securities and Exchange Commission, and remote branches and trading floors to connect to the NSE's DR facility.
  - The network connectivity target is 100%.
  - The LAN or WAN must be capable of supporting the transaction volumes generated by the application software based on the trading and settlement volumes of the NSE.
  - The network must conform to international standards.
  - The network must be capable of expanding to accommodate future growth of participants and transaction volume.
  - The network must be flexible to enable the addition of:
    - extra communication links,
    - extra processing power for network nodes
    - new network nodes and
    - the relocation or expansion of existing nodes.
- **Ensure that the network design will allow the network to operate even if communications links become unavailable.**
- **The DR data center network must incorporate remote access capabilities that will allow trading from the other regional branches and trading floors to continue. This may include:**
  - Remote Access Server (RAS)
  - Any end user in any office to access the trading and settlement systems
  - The transmission of electronic mail to any registered user on the network.

- **Ensure that the network design identifies the data protocols and data transfers over the network and the internet.**
- **Ensure that the network design defines the circuits that must be installed in order to:**
  - Handle the data replication traffic as well as
  - Handle a minimum of 50% of the current production load and throughput.
- **Ensure that the network design defines the types of communication and telecommunication connectivity required to:**
  - Support connectivity to the facility
  - Routers and multiplex equipment needed for navigating network traffic
    - Tl leased lines,
    - VSAT or
    - Fiber optics.
- **Ensure that the network design defines the equipment to switch over to the backup data communication link using a minimum of 56Kbps dial-up lines and can support:**
  - The maximum data throughput between all major sub systems and components.
  - Both LAN and WAN throughput.
- **The DR data center network must incorporate a network management system that:**
  - Covers the entire network
  - Provides line-loading, performance, and error and throughput measurement
  - Continuous aggregate figures on data throughput between all nodes
  - Potential difficulties can be predicted and preventive maintenance performed.
- **The DR data center network must define the data transmission on the internal and external networks to:**
  - Support authentication of network terminals and workstations
  - Prevent unauthorized monitoring of network transactions
  - Support encryption I decryption techniques
  - Define a file transfer system for error free transfer between systems
  - Logging of file transfer requests, actions and failures
  - Utilize international transfer protocols.

Power Consumption.

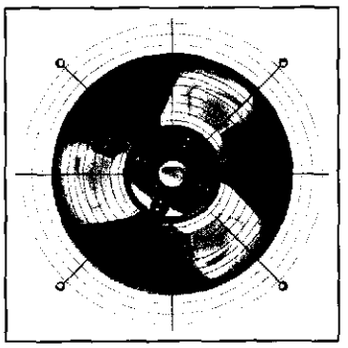
GIT researched and evaluated the criteria for the power consumption needed for the NSE DR.

To achieve this, GIT recommends that:

- **The power equipment required for the DR facility must ensure that all processors, disks and communications equipment require computer-grade automatic voltage regulators with:**
  - 220-volt 50-Hertz power supply
  - Automatic shutdown circuits in case of unit failure,
  - A maximum of 1 nanosecond response time.
- **Ensure that the power consumption needs incorporate power generators:**
  - For the full facility as well as
  - Duplicate backup generators for the building.
- **Ensure that the power consumption needs include in power requirements**
  - A main uninterruptible power supply (UPS) to support the data center
  - A duplicate UPS for manual failover.
- **Ensure that the power consumption needs support stabilizers for the data centers and the workstations.**
- **Ensure that the power consumption needs address:**
  - Voltage and voltage tolerance requirements,
  - Total power consumption,
  - Electrical grounding requirements,
  - Conductor sizes, and
  - Any other special requirements.
- **Ensure that the power consumption needs includes the number of power outlets**
  - At the central site and
  - At participants' offices.

Note: Additional Resource Requirements and Needs as well as Actions & Related Emergency Procedures are identified and described in Appendix 7, 10 and 11.

Cooling Capabilities.



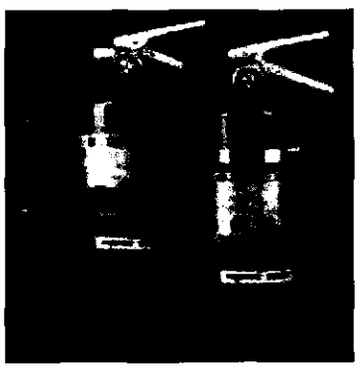
GIT researched and evaluated the criteria for the cooling needs for the NSE DR.

GIT recommends that:

- **Ensure that the cooling capabilities at the DR facility and the equipment procured allow for comfortably sustaining:**
  - An optimum inside temperature of 68 degrees (F) with
  - A maximum external temperature of 120 degrees (F). :
- **The cooling capabilities at the DR facility include:**
  - Prolonged and strong air conditioning and
  - Ventilation in the building.

Note: Additional Resource Requirements and Needs as well as Actions & Related Emergency Procedures are identified and described in Appendix 7, 10 and 11.

Fire Protection.



GIT researched and evaluated the criteria for the Fire Protection needs for the NSE DR facility.

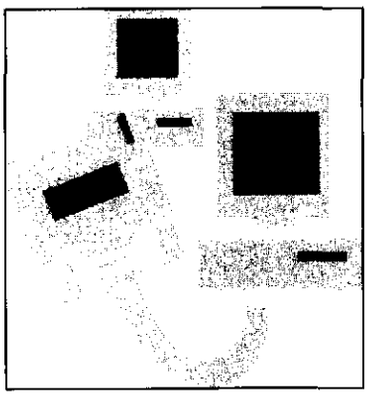
GIT recommends that:

- **There must be adequate running water in the DR facility building as well as the neighboring area**
- **There must be adequate training to educate and train the personnel in**
  - Fire safety,
  - Emergency procedures
  - Handling of necessary fire extinguishers and
  - Other safety equipment depending on the type of system.
- **There must be an adequate number of fire extinguishers in place in the rooms and hallways of the DR facility building. In each such case:**
  - Portable fire extinguishers must be mounted, located and identified so that they are readily accessible to employees without subjecting the employees to possible injury.
  - The portable fire extinguishers must use carbon tetrachloride or chlorobromomethane extinguishing agents.
  - The portable fire extinguishers must be maintained in a fully charged and operable condition and kept in their designated places at all times except during use.
- **The fire extinguishers must be placed consistently throughout the DR facility.**
- **Portable fire extinguishers must be distributed based on the classes of anticipated workplace fires and on the size and degree of hazard which would affect their use.**
  - The distribution of portable fire extinguishers for use on Class A fires so that the travel distance for employees to any extinguisher is 75 feet (22.9 m) or less.
  - The use uniformly spaced standpipe systems or hose stations connected to a sprinkler system installed for emergency use instead of Class A portable fire extinguishers, provided that such systems meet the respective requirements must provide total coverage of the area to be protected, and that employees are trained at least annually in their use.

- The distribution of portable fire extinguishers for use on Class B fires so that the travel distance from the Class B hazard area to any extinguisher is 50 feet (15.2 m) or less.
- The distribution of portable fire extinguishers used for Class C hazards on the basis of the appropriate pattern for the existing Class A or Class B hazards.
- The distribution of portable fire extinguishers or other containers of Class D extinguishing agent for use so that the travel distance from the combustible metal working area to any extinguishing agent is 75 feet (22.9 m) or less.
- Portable fire extinguishers for Class D hazards are required in those combustible metal working areas where combustible metal powders, flakes, shavings, or similarly sized products are generated at least once every two weeks.

Note: Additional Resource Requirements and Needs as well as Emergency Procedures related to Fire Fighting, Fire Reporting and Fire Safety are addressed in Appendix 7, 10 and 11.

Data Replication.



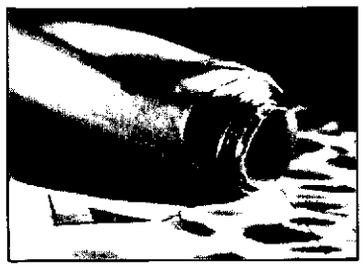
GIT researched and evaluated the criteria for the Data Replication needs for the NSE DR facility.

GIT recommends that:

- **The information must be provided with respect to synchronous ongoing real time data replication**
- **The proposed location for the DR facility must be within 20 cable miles of the current *NSE/CSCS* location.**
- **Select data replication method from Oracle replication, EMC SRDF, SQL Log Shipping.**
- **Perform daily updates via web**
  - Consider alternative type and media for the daily updates that also include tapes and diskettes
- **Perform weekly updates via tape**
  - Consider alternative type and media for the weekly updates that includes diskettes or via the web.

Note: Additional Resource Requirements and Needs as well as Actions & Related Emergency Procedures are identified and described in Appendix 7, 10 and 11.

Site Plan.



GIT researched and evaluated the criteria for the Site Plan needs for the NSE DR facility.

GIT recommends that the type of facility, construction details, location, as well as building logistics must align with the DR facility requirements:

- **The DR facility must be a secure facility that has its own generators, stabilizers, UPS, running water, guards and security-controlled building access.**
  - Alternatively, the additions or modifications can be applied to an existing facility such as the CSCS DR facility in Ikoyi, Lagos.
  - If a new building is required, the building should be in mainland Lagos.
- **Ensure that the DR facility includes any special needs such as steel reinforcement of the roof. etc.**
- **Ensure that the DR facility includes the power and telephone lines requirements for the facility.**
- **Ensure that the DR facility is supported by emergency procedures and the training (see Appendix 10, 11) necessary to:**
  - Enable the NSE and CSCS staff to react and operate in reduced capacity
  - Define the functions of the technical staff and training required to operate the equipment and DR failover and provide emergency support.
  - Define the contingency and business continuity strategy for mission-critical business operations and systems, including trading applications, trading processes. equipment and mission-critical staff.
  - Define the type of personnel and the necessary skills and qualifications required to successfully establish and maintain an emergency response DR system.
  - Define a target schedule for practice of emergency procedures.

IMPLEMENTATION PLAN

The GIT focus was to create a phased implementation plan for the DR facility that supports creation of a procurement schedule for all facility elements.

Task & Deliverable Summary

Taking into account the DR Strategic Plan, GIT created a phased implementation plan for the DR facility highlighting seven (7) broad project Phases, related Tasks and associated Deliverables:

- Complete DR Plan
- NSE Data Completed
- Supplier RFQ/RFP
- Vendor(s) Selection
- Build & Acquire
- Load & Test
- Management Review

The final implementation phase is followed by a recurring "Fire Drill" (or Test) phase/task to ensure that the DR Plan remains accurate, reflective and relevant to the NSE facilities.

NSE Work Plan Details

GIT documented each of the main tasks and the scope of work with start and ending estimates (See Appendix 8).

The Implementation Plan is currently estimated to require over 550 elapsed days to complete.

> **Note**: This estimate will be modified based on Vendor responses to the RFP process and the time required for the Build & Acquire phase.)

In addition, the structure of the plan facilitates the (optional) use of an automated project management system by NSE.

The NSE DR Implementation Work Plan facilitates:

- Guidance for planning
- A basis for managing the ongoing efforts

Implementation Plan Effort Estimates and Schedule

The Facility Plan identifies initial effort estimates for each project task.

In addition the project plan provides a series of phase level duration estimatess that are structured using a number of days relative to "0" which is the start of the project. In this way date slippages do not require plan regeneration.

Premises & Assumptions

The Implementation Plan schedule and dependencies were prepared based on the following premises and assumptions:

- Project Tasks and Deliverables are based on the content of this DR Facility Plan, Procedures & Specification
  - GIT also reviewed and referenced the project design, deployment and business model components of Appendix 13 - the DRP of the National Stock Exchange of Mumbai
- "RESP" – identifies broad Responsibilities within the NSE and various Suppliers and Vendors
  - Plan should be amended with specific groups as they are identified
  - Note: NSE functional names rather than personal names should be used to minimize changes as individuals join and/or leave the organization or change titles or responsibilities
- Status codes are color coded to facilitate ease of status reporting
  - The "STATUS & COMMENTS" fields are "grayed out for planning and should be colored with the appropriate color where:

Green = In Progress & On Schedule
Yellow = Potentially Behind Schedule
Red = Off Schedule
Blue = Complete
White = Not Started & On Schedule

- The "DUE" column identifies the number of work days starting from "0" – which is the start dates of the project
  - This allows NSE to use the plan without constant modifications based on the variations that may occur in the project start date as well as any project delays

Roles and Responsibilities

This section defines the responsibilities for to help ensure NSE business continuation. Responsible areas and individuals will be held accountable for compliance with the standards (See Appendix 9) based on reasonable, cost effective approaches for implementation.

> **Note:** The DR Roles and Responsibilities have been grouped consistent with the NSE organization structure. However, the actual NSE functional responsibilities and reporting structure may vary.

Market Operations Related

Business Group Executive

Role: Business Group Executives are responsible for ensuring that approved business continuation plans are developed, tested and maintained for critical functions within their area of responsibility. It is recommended that the Business Group Executive appoint the Business Continuation Officer(s) for their group.

Risk Management & Regulation Related

Business Continuation Officer

Role: The Business Continuation Officer is responsible for managing all aspects of the business continuation function within their line(s) of business, including the coordination of the business group's continuation planning process in accordance with Enterprise planning standards. The Officer is also responsible for ensuring that all business units within their lines of business develop business continuation plans or submit plan waivers in accordance with Enterprise standards. The Business Continuation Officer is appointed by and reports directly to one or more members of the Senior Management Group and serves as a counselor to management on matters of business continuation, risk preventive measures, BC costs, and all other BC related issues.

Business Continuation Coordinator

Role: The Business Continuation Coordinator is the backup for the Business Continuation Officer. The Coordinator is responsible for coordinating the development, maintenance and testing of plans with planners within their line(s) of business in accordance with company planning standards. The Business Continuation Coordinator is appointed by members of the Senior Management Group and the Business Continuation Officer. The Business Continuation Coordinator reports directly to the Business Continuation Officer and serves as counselor to the Officer on matters of business continuity, risk preventive measures, BC costs, and all other BC related issues.

Business Continuation Planner

Role: BC Planners are responsible for writing, testing and maintaining the business continuation plan(s) for their respective function(s). A business group may have many Business Continuation Planners depending upon the number of sites and the complexity of the critical business functions that need to be protected. Business Continuation Planners will work closely with their unit's Business Continuation Officer in their planning efforts. The BC Planner is appointed by Division Management with approval of Senior Management. In selecting candidates, appropriate skill sets should be considered. Where appropriate, the Business Group may appoint assistant planners based on the needs of the organization. This relationship may be considered a matrix managed reporting line to the Business Group BC Officer according to their Business Group reporting relationships.

Enterprise Business Continuation Office

Role: The Enterprise Business Continuation Office**Error! Reference source not found.** (EBCO) is the corporate and business level group responsible for Enterprise-wide oversight of the TPG Business Continuation Program.

Management Internal Control

Role: Management Internal Control (MIC**Error! Reference source not found.**) is responsible for supporting business and corporate units in the design, implementation, and ongoing monitoring of TPG's system of internal controls.

Corporate Records Management

Role: The Corporate Records Management Department is responsible for developing, implementing and managing the Enterprise-wide Records Management Program which deals with the control of records throughout their entire life cycle (from original creation or receipt through active reference, inactive storage, and final disposition).

Legal

Role: The Law Department is responsible for advising and working with business units to implement the process by which changes in laws and regulations are tracked, evaluating those changes based on their applicability to TPG, and communicating them effectively throughout the Enterprise. The Law Department maintains its principal role as the interpreter of all laws and regulations for the Enterprise and its business and corporate units.

Corporate Risk Management

Role: Risk Management is the corporate level group responsible for the development and placement of risk financing programs for the Enterprise and its subsidiaries. The major Enterprise-wide programs include Property (buildings & contents), Casualty (liability insurance), and Executive risk.

Internal Audit

Role: TPG's Internal Audit Division performs independent appraisal activities to serve the Auditing Committee of the Board of Directors. Procedures are independently analyzed and tested to ascertain that adequate controls are established and function as intended to detect abuses or conditions that might result in the loss of assets, circumvention of policies and instructions, inaccurate reporting of results, inefficient use of resources, or embarrassment to the Enterprise.

Information Technology & Market Operations Related

Technology Support Services

Role: Technology Support Services is the general title applied to any group that contracts with TPG business groups to provide technology-related services including technology acquisition and line-of-business and corporate infrastructure (voice and data support, desktop support, LAN administration, mainframe support, etc.).

HR & Real Estate Related

Human Resources

Role: Human Resources is the corporate level group that manages personnel issues.

Property Manager

Role: The Property Manager's business continuation responsibilities (during planning, during an incident, and post-incident) relate primarily to emergency preparedness, tenant safety considerations, and incident response actions.

Corporate Real Estate

Role: Assumes an Enterprise-wide oversight role for both TPG owned and leased properties. Coordinates risk and recovery assessment activities for owned properties and provides oversight and risk and recovery assessment consultation for leased properties.

Purchasing Operations/Administrative Services

Roles: The procurement team handles travel, mail services, food services, and purchasing of materials, supplies, and non-technology office equipment during an emergency incident.

Corporate Public Relations

Role: Coordinates all internal and external communications during and following an emergency, including communications to employees, clients, customers, investors and the public.

NSE SUPPLIERS AND IMPACT RESULTS

Supplier Identification

GIT worked with NSE to identify potential suppliers of computer software and hardware and services in both Nigeria and the United Staes.

This information is needed in sufficient detail that the NSE can make informed, responsible decisions regarding product or service procurement.

Nigerian Suppliers

NAME	FOCUS	CONTACT
Progenics Corporation Limited 50/52 Toyin Street P.M.B. 21010 Lagos, Nigeria	International banking and remote access software	234 (1) 2703341 www.progenicscorp.com
Allied Soft Nigeria Limited Plot 5B Charles Ifeanyi Street Off Road 14, Lekki Phase 1 Lagos, Nigeria	HR and Payroll software	234 (1) 2703341 www.alliedsoftng.com
InfoSoft Nigeria Limited 99 Opebi Road Ikeja, Nigeria	IT Professional Services firm	234 (1) 493-7335 www.infosoftconsulting.com
Global InfoSwift Technologies Limited (GIS) 96, Awolow Road Ikoyi - South West Lagos, Nigeria	IT Professional Services firm	234-1-2704676 www.globalinfoswift.com
Dimension Data 57 Sloane Street Corner Sloane Street and Main Road Bryanston, Johannesburg 2021	Network solutions firm	271 (1) 575-0000 www.dimensiondata.com
TelNet Nigeria Limited	Telecom and network	234 (1) 4611747

NAME	FOCUS	CONTACT
Plot 242 Kofo Abayomi Street Victoria Island, Nigeria	solutions firm	www.telnetng.com
Net Solutions Limited Plot 213A Muri Okunola Street Victoria Island, Nigeria	Network and Telecom Hardware and Services	234 (1) 2701441 www.netsolutionsltd.com
Chartered Institute of Stock Brokers (CIS Niugeria) (10th Floor, CSS Bookshop House 50/52 Broad Street Lagos, Nigeria	A training and certification firm	234 (1) 280-2180-5 www.cisnigeria.com
Computer Warehouse 5th Floor, Octagon Building 13A, J Marinho Drive Victoria Island, Nigeria	Reseller and Installer of Hardware, Telecom and Networks	234 (1) 2704674-5 www.cwlgroup.com
Kecam Ventures 49B, Oluwaleyimu Street Allen Avenue, Ikeja Legos, Nigeria	Reseller and Installer of Hardware, Telecom and Networks	234 (1) 8131269 www.kecamventures.com
Right Click Nigeria 29 Ogunlowo Street, Ikeja Lagos, Nigeria	Decision Support Solutions	234 (1) 7379558 www.rightclick-ng.com

United States Suppliers

NAME	FOCUS	CONTACT
Oracle Corporation 500 Oracle Parkway Redwood, Shores, CA 94065	Enterprise software developer	(650) 506-7000 www.oracle.com
CSI Complex Systems, Inc. One Exchange Place, 8th Floor Jersey City, NJ	Trade and finance software products	(201) 435-1490 www.banktrade.com

NAME	FOCUS	CONTACT
New Dawn Technologies 843 South 100 West Logan, Utah 84321	Department of Justice case management software	(435) 713-2100 www.newdatatech.com
Intermark Solutions 866 United Nations Plaza Suite 566 New York, NY 10017	Front, middle and back office brokerage software	(212) 223-3552 www.intermarkit.com
Computer Associates One CA Plaza Islandia, NY 11749	Software/Hardware Manufacturer	(800) 225-5224 www.ca.com
IBM One New Orchard Road Armonk, NY 10504-1722	Software/Hardware Manufacturer	(914) 499-1900 www.ibm.com
Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134	Software/Hardware Manufacturer	(800) 553-2447 www.cisco.com
Hewlett-Packard 3000 Hanover Street Palo Alto, CA 94304	Software/Hardware Manufacturer	(650) 857-1501 www.hp.com
Oracle/Sun Microsystems 500 Oracle Parkway Redwood Shores, CA 94065	Software/Hardware Manufacturer	(650) 506-7900 www.oracle.com
Global Information Technology (GIT) 8913 Regents Park Drive Suite 670 Tampa, FL 33647	IT Professional Services firm	(813) 973-1061 x228 www.git-org.com

Development Impact Analysis

GIT determined the potential development impacts for the project in the Host Country of Nigeria.

Once the NSE successfully operates a true disaster recovery and business continuity management culture, NSE will:

- Have Systems that are more effective, more efficient, more nationally and internationally utilized than competitors.
- Be able to maximize the return on investment (for The NSE and partners) have made in business processes.
- Be more productive, more reliable and an excellent partner and service provider.
- Set and meet deadlines
- Undertake a project and will deliver on time and on budget.

In this way, business continuity management becomes necessary not because it means NSE will survive into the distant future; but because it will make NSE a better and more competitive business today for all their stakeholders.

In addition, NSE will be able to:

- Analyze the impact of a business disruption and the cost of downtime, then assess and address any gaps.
- Manage risk through an enterprise-wide resiliency strategy
- Reduce cost through proactive incident response and reduced downtime
- Ensure resilient service delivery in a 24-hour, 7-day-a-week world
- Respond with speed and agility while minimizing risk exposure

Development Benefits Analysis

GIT determined the potential development benefits for the NSE project in Nigeria. These include:

Security Benefits

- Ensure your data is effectively backed up and easily recovered.
- Protect valuable information assets: Prevent loss of business information from site disasters, viruses, human error, and application and system failures by providing alternate remote and local copies of data and enabling rapid restart and recovery.

- Consolidation is perhaps the most obvious and popular means of enhancing IT service levels while simultaneously improving controls as well as lowering costs.

Reliability Benefits

- Assess how you can reinforce your business processes so that when unexpected disruptive events occur, NSE customers and NSE partners remain in contact and your brand stays strong
- Enable NSE workforce to continue working in times of disruption.
- Protect the NSE brand through industry-leading disaster response and recovery platform and processes
- Having a top-quality, tried and tested disaster recovery and business continuity management structure in place will help the NSE stand out from others.

Data Integrity Benefits

- Deployment of a solid DR/BC management structure and infrastructure guarantees availability of data that is less prone to corruption, manipulation and loss.

Other Benefits

- Determine the constantly changing governmental and industry regulations associated with business continuity that apply to you and help develop a plan for compliance.
- Standardize IT practices on fewer storage platforms: Gain improved performance and greater scalability and availability; reduce burdens on IT staff
- It can help to create a business that operates its systems to the optimum level. Business continuity management involves creating resilient businesses; companies that are flexible and which can quickly identify and respond to challenges and threats. However, resiliency is not just a benefit in times of disaster. Resiliency can provide day-to-day business benefits with hardened systems failing less often and production returning more quickly from day-to-day

glitches than would be the case in less resilient businesses. In other words, business continuity management is about optimizing process availability; and this enables businesses to operate to maximum efficiency at all times.

Project Benefit Estimate

GIT estimated the potential development benefits for the NSE project in Nigeria. These include:

Infrastructure / Industry

- Veritable platform for the capital market
- Further strengthen positive perception of the market
- Increase in investor confidence in the market
- Enthrones best practice for other arms of the market to follow
- Drive growth in the industry
- Positions the market to attract more FDIs
- Prepares the Stock Exchange to join the league of global players
- The business that recovers most quickly from a wide-area disaster is the business which is able to capitalize on the situation. Disasters create new markets and open up existing ones. This may allow the rapid development and launch of new products

GIT reviewed and determined that there will be no impact on any regulations, laws, or that any institutional changes will be needed.

The areas reviewed to determine areas of potential need and any recommendations as well as the affect they would have if implemented include:

Market-Oriented Reforms

- This will further support current reforms and transformation programs already embarked by both The Stock Exchange and SEC
- It will fall in line with recommendations made for market improvement in the areas of enhanced information availability and integrity of data.

- It will guarantee transparency and fairness in the market which will translate into investor confidence
- It is well documented that an effective disaster response can help a company's share price to increase and its reputation to become stronger. Therefore the project will enhance perception of The NSE and positive impact on our overall rating as a market and organization

GIT estimated the number and type of positions that would be needed to implement, manage, and operate the proposed Project in terms of how many people will receive training and what kind of training program would be needed. GIT determined:

Human Capacity Building

End User Training will involve educating every one of their roles during a DR/BC operation and their roles in maintaining preparedness for any eventuality

- Three types of training will be conducted, namely: Technical, Operational and End User Trainings.
- Technical Training will focus on the architecture, infrastructure and configuration of the various platforms to be deployed for the DR/BC.
- Operational Training will focus on day to day procedures and management of the DR/BC procedures and maintenance of a continuous state of preparedness.

GIT identified any advanced technologies that will be implemented as a result of the Project to determine the type(s) of productivity and efficiency gains that might result.

Technology Transfer and Productivity

- Increased WAN capacity and WAN upgrades
- Adequate training and mentoring must be put in place to ensure knowledge transfer and sustainability of all processes and procedures
- Regular knowledge updates and technology upgrades must be part of the maintenance and support agreement with the vendors.

- Productivity will result through reduction or elimination of downtime, access to data and information will be available to all stakeholders thereby increasing task completion and eliminating reworks and unnecessary errors, misrepresentation and correction

Use resources and personnel efficiently: Offload processing and data to alternate systems and locations; use advanced software tools to minimize the labor intensive nature of backup and recovery procedures

GIT determined any other developmental benefits of the Project, including any spin-off or demonstration effects

Other.

- Simplify disaster recovery: Achieve rapid restart/recovery over virtually any distance with minimal impact on application response time; eliminate inefficient and resource intensive tape-based replication or retrieval systems

GIT determined with NSE help that there are no potential adverse environmental impact to local requirements and those of the World Bank

APPENDIX

There a number of items that have been placed in the Appendix due to their size or to minimize disruption to the flow of the overall report.

The Appendix contains:

1. NSE BCP/DRP Project Questionnaire
2. Letter of Invitation
3. NSE Network Diagrams and Resources
4. NSE BCP/DRP Disaster And Contingency Plan Process
5. Decisions related to Failover vs. Backup
6. NSE Emergency Team Composition
7. NSE Resources
8. NSE Implementation Work Plan
9. NSE BCP Standards
10. NSE BCP Plan, Emergency Actions & Procedures
11. NSE DR Response & Recovery Checklist
12. Sample – NSE Disaster Recovery Procedure Guide
13. Sample - Mumbai DRP
14. NSE Supplier & Impact Questionnaire/Response
15. The Nigerian Stock Exchange Proposed Organization Plan & Charts
16. NSE BCP/DRP Project Questionnaire Response
17. NSE Disaster Recovery and Systems Backup Project Technical Assistance

18. NSE Original Analysis

Each component of the Appendix is depicted and described throughout the remaining pages.

APPENDIX 1

1. NSE BCP/DRP Project Questionnaire

Your Name:		**Title:**	
Job Function		**Reports to:**	
Date:			

Background

This Questionnaire Guide is used to determine your input into the NSE Disaster Recovery Planning & Business Continuity Planning project.

The DRP will provide a mechanism for continuous trading and support of the NSE in case of failure of the main building or main equipment and ensure that the data stored and transferred on the NSE's hardware and communications infrastructure is fully recoverable and secure.

The Technical Assistance will include the review of existing IT systems and plans, existing hardware and communications infrastructure, and would develop a strategic plan, specifications, and an implementation plan for a disaster recovery facility. The Technical Assistance will also ensure that any recommended procurements can be integrated with existing hardware, communications infrastructure, applications, and databases.

The data gathered will form the basis for comparison to industry-based Disaster Recovery Planning Best Practices. A Gap Analysis will be documented as a critical component of the "NSE DR As-Is Assessment" delivered to NSE.

GIT will utilize the Gap Analysis and DR Assessment along with the DR Best Practices and its extensive experience to develop and document the critical procedures, forms and reports that will be integrated into an overall NSE DR Facility Development Plan.

This Guide is made up of a number of questions in five (5) broad areas pertaining to information that we have found to be important to the successful implementation of the NSE DRP. These include:

- **Current NSE Environment**
- **NSE Emergency Response Procedures**
- **NSE DR Plan Activation Procedures**
- **NSE Administrative Procedures**

- **NSE DR Reports & Forms**

At the end of each section is an area to provide any general Comments that you may have about the overall section.

GENERAL INSTRUCTIONS

Enter the information that "best" represents your specific understanding about the Disaster Recovery and Business Continuation needs for NSE. Add extra information wherever necessary – attach any information requested.

If you create a "soft-copy," create a "Save As" copy using your Initials and the date. For Example: IB-2-20 NSE Q v 1.0"

CIRCLE your answer to each question. Please do not guess: if you don't know the answer, don't respond to the question. Keep in mind that you can identify that you "Don't Know" (DK) for any question area(s) that do not apply to your job, or where you have no direct information.

Please enter as much clarifying information as you can.

Note: All of the information entered this questionnaire will be held in strict confidence.

PLEASE RETURN THE COMPLETED GUIDE FILE WITHIN ONE WEEK AFTER YOU RECEIVE IT

Next Steps:

1. **Complete the Questionnaire and return both paper AND "soft"-copy)**
2. **The GIT project team will consolidate Results**
3. **The GIT project team will Report back to You and all Stakeholders with a draft DRP**
4. **The GIT project team will develop the final DRP and present to NSE**
5. **The GIT project team will continue to work with you.**

If you have any questions, please call or contact:

- **Mike Ike 901-218-6233 or**
- **Irv Brownstein at 908-872-8139.**

Thank You!!

CURRENT NSE ENVIRONMENT

	Is there an NSE Disaster Recovery (DR) POLICY Statement? YES or NO or DK (Don't Know)
	If YES, Please Attach

	Is there a current DR PLAN? YES or NO or DK
	If YES, Please Attach

Identify the INDIVIDUALS to be contacted In case of emergency

Immediately Notify The Key Emergency Contacts Listed Below:

Contact	Office Number	Home / Mobile Phone
Security Desk		

In the event that none of the above key contacts are available, call .

Who must APPROVE the Disaster/Recovery Plan? List All individuals

Name	Title/Function

	Is there a FAIL-OVER SITE? YES or NO or DK
	If Yes, Do you have a current Fail-Over site agreement? (ATTACH) Date executed? _____ Does the Fail-over site have the same • Software? YES or NO - IF YES, ATTACH LIST • Supplies? YES or NO IF YES, ATTACH LIST Has the Site been tested in a formal fire-drill? YES or NO • If YES, When? _____ • IF YES, What results? (ATTACH RESULTS)

	What are the current NSE processing VOLUMES?
	For each Transaction type – identify the Volume, Period, Peak period volumes Identify the general volume history over the past 24 months (or attach separate report covering the same data).

Month	Daily Volume	Peak Volume (hours)	Comment

	Identify the failure history over the past 18 months. In each case detail each outage using the following table (or attach separate report covering the same data).

Date	Duration	Impact/Extent	Cause / Comment

Identify the KEY CONTACT INFORMATION related to each critical business function? List All individuals

Function Name	Name & Title/& Contact Information

List all software used to support NSE (List Below Or Attach Report)

Name	Vendor/supplier	Version/release	Use

Identify the current NETWORK for both data and telecommunications

Provide one or more systems architecture chart(s) that highlights each element of the

- IT Infrastructure depicting each device type
- Telecommunications protocols

Describe BUSINESS UNIT INVOLVEMENT with the NSE DR

How many people are involved from your business units in BCP planning?

Are they accountable for plan content development and approval?

Do they participate in testing exercises?

	Describe NSE SECURITY related to the NSE DR
	Do you have fulltime security personnel? Are they included in your BC/DR plans? Have you defined predefined roles during an outage?

	Identify the NSE EXECUTIVE SPONSORSHIP
	Who is responsible for Business Continuity Planning? What is the organizational structure? Do you have a steering committee of representatives? How frequently do they review plan readiness and issues? If you have a board of directors, is BCP reviewed?

	Describe NSE RISK ASSESSMENT
	Do you perform routine facility risk assessments? Do you meet with local fire, police, and Hazardous Material teams to ensure assumptions in plan are within their guidance? Have you identified internal and external threats? Do you have controls in place to monitor Security, Life Safety, and Communication to Personnel? Have you developed risk exposures and financial cost analysis?

COMMENTS:

NSE EMERGENCY RESPONSE PROCEDURES

Emergency response ensures that all parties act to quickly determine the emergency and take appropriate action. GIT will complete this stage of the project in three tasks:

- Emergency Evacuation Procedures
- Emergency Phone Numbers
- Emergency Notification Procedures.

A business disruption has three distinct phases: Emergency, Recovery, and Restoration. The emergency operations center (EOC) is the focal point of communication and coordination for resources during a business disruption.

	Is there an EMERGENCY MANAGEMENT TEAM? YES or NO or DK
	If YES Please describe or attach

	Is there an EMERGENCY OPERATION CENTER? YES or NO or DK
	If YES Please describe or attach

	Are there documented EMERGENCY PROCEDURES? YES or NO or DK
	If YES is there a chart that outlines the procedure steps that address notification and mobilization (Please attach)? Identify in the table below (or attach) the procedures that indicate what steps are followed AND who (Name & Title) is responsible for the specific actions.

Step	ACTION/PROCEDURES	WHO
1		
2		

	Identify the current NSE EMERGENCY CONTACT LIST

Notified By	EMT Role	EMT Member Name	Numbers
	EMT Leader		

H = home W = work C = cellular S = satellite F = fax

COMMENTS:

NSE DR PLAN ACTIVATION PROCEDURES

Plan activation ensures that all parties and all materials are coordinated for the DR Facility. GIT will complete this stage of the project in ten (10) tasks:

- Activate Incident Management Team
- Activate Emergency Operations Center
- Emergency Declaration Procedures
- Relocate Operations Procedures
- Situation & Damage Assessment Procedures
- Communications
- Offsite Storage

- Purchasing procedures
- Recovery Site Generator, Electrical & Security plan Procedures
- Reconstruction Procedures

Identify the Mission CRITICAL BUSINESS FUNCTIONS AND PROCESSES

For each critical function service, product and/or system identify the time-frame (Notification and Recovery) that it must be fully operational (Note: use additional pages as necessary)

Critical Business System Function/Process	Recovery Time Objective
	Notification: Recovery:
	Notification: Recovery:
	Notification: Recovery:
	Notification: Recovery:
	Notification: Recovery:

Note: All recovery time objectives, other than immediate, reflect business days or weeks.

Are there RECOVERY STRATEGIES Associated With All Or Any Business Segment Or Function? YES or NO

I. TRANSFER OF WORK	
Approach	**Responsibility**
II. IN HOUSE RECOVERY	
Approach	**Responsibility**

III. WORK FROM HOME	
Approach	**Responsibility**

Is there a defined RECOVERY ORGANIZATION? YES or NO

If YES Please describe or attach

Name	Function

If YES, what are their ROLES AND RESPONSIBILITIES (Describe or attach)

Function	Role	Responsibilities

This section identifies the specific procedures for Disaster Recovery Teams to follow during the various stages of a disaster.

Identify and describe tbe Procedure Steps for the EMERGENCY PHASE (or attach)

Identify in the table below (or attach) the procedures that indicate what steps are followed AND who (Name & Title) is responsible for the specific actions.

Step	ACTION/PROCEDURES	WHO
1		
2		

Identify and describe the Procedure Steps for the RECOVERY PHASE (or attach)

Identify in the table below (or attach) the procedures that indicate what steps are followed AND who (Name & Title) is responsible for the specific actions.

Step	ACTION/PROCEDURES	WHO
1		
2		
3		

Identify and describe the Procedure Steps for the RESTORATION PHASE (or attach)

Identify in the table below (or attach) the procedures that indicate what steps are followed AND who (Name & Title) is responsible for the specific actions.

Step	ACTION/PROCEDURES	WHO
1		
2		
3		

Identify the RESOURCES - Software, Hardware and Supplies associated with the procedures

Include (or attach) references to space, specific supplies, software names and versions, hardware devices

Item	Description and Use

COMMENTS:

NSE ADMINISTRATIVE PROCEDURES

The administrative responsibilities summarize NSE policy. These responsibilities and procedural guidelines must be applied throughout the initial response and any subsequent business recovery activities.

- Enforce NSE Policies
- Monitor & Report Recovery process
- Maintain Recovery Related Record Keeping
- Define Testing & Maintenance Functions

	Is There A Defined MAINTENANCE SCHEDULE (Describe Below Or Attach)? YES or NO or DK

	What Events Trigger A MAINTENANCE REVIEW?
	The following table includes many events that may necessitate a maintenance review.

Situation	**Actions Taken**

	Are DISASTER RECOVERY PLAN UPDATES Made On A Scheduled Basis? YES or NO or DK
	Yes – Describe And Identify The Distribution

	Are there DIRECTIONS to Emergency Operations Centers? YES or NO or DK

	How are Policies ENFORCED? (Describe Below Or Attach)

	How is Record Keeping MAINTAINED? (Describe Below Or Attach)?

	Is there a DAMAGE ASSESSMENT CHECKLIST? (See Sample) YES or NO or DK
	If Yes – Describe or attach

	Is there a FACILITIES EMERGENCY PROCEDURES? YES or NO or DK
	If Yes – Describe or attach

	Is there an ORGANIZATION CHART with a Master Employee Listing? YES or NO or DK
	If Yes – Describe or attach How frequently is your call tree updated?

	Is there a RECOVERY STATUS REPORT? (See Sample) YES or NO or DK
	If Yes – Describe or attach

	Is there an APPROVED PRESS RELEASE? (See Sample) YES or NO or DK
	If Yes – Describe or attach

	Is there a MAINTENANCE LOG? YES or NO or DK
	If Yes – Describe or attach

	Describe the NSE Profile
	How long has NSE been in business? How many locations does NSE have? What is the number of people by location? How many people are within NSE overall? Please define the organizational structural by business unit?

	What percent of the NSE budget is dedicated towards BCP? Does NSE currently have a BCP Steering Committee? Who are NSE's primary client(s)? Where are they located?

	How is Client COMMUNICATION handled about NSE "Disasters"?
	What is communicated to your clients concerning BCP? Do you track what was said and to whom? Do you receive inquiries from clients? Do clients ask for onsite visits? Do you have a centralized repository for issue management? Who is overseeing closure of critical issues? Do you utilize any tools for mass communication? Do you utilize your website? How do you to communicate to personnel during a situation? How frequently do you communicate plans status, evacuation plans, and life safety preparedness to your personnel? Do you have a plan to communicate to external vendors and clients? Have you tested this? When and What was the result?

	Identify the NSE DR PROGRAM CONTROLS
	How do you monitor your plan readiness? What metrics do you use for testing of plan content? What percent of people participate in business unit testing?

	Do you review your program with Legal/Compliance teams?

	Discuss NSE DR PROGRAM MATURITY
	Have you instituted a firm-wide plan for business continuity?
	Are key members of your businesses involved?
	What percent of BCP activities are completed with Information Technology?

	Describe NSE LIFE SAFETY related to the NSE DR
	Do you have first aid responders within your buildings?
	What is the frequency of their training?
	Do you personnel know who they are and how to engage with them?
	Do you they have role within the Incident Management Plan?

	Describe NSE INCIDENT MANAGEMENT PROGRAM related to the NSE DR
	Do you include life safety, security, business units, and IT in your incident management program?
	Do you have a location near the building for people to gather in a evacuation?
	Do you have a mechanism to verify all people have safely left the building?
	Do you have a Incident Manager for each site in your organization?
	Do you have a checklist for that person to execute and provide status?
	Have roles and responsibilities been clearly assigned for during the event?

	Describe NSE INDUSTRY TESTING related to the NSE DR

	Do you participate in industry testing? Do you test with your critical vendors? What level of participation is required? How frequently do you test?

	Describe NSE BACKUP SITE INVOCATION PLANS related to the NSE DR
	Do you have steps to activate your backup site? Do they include communication, transportation, and logistics? Do you have decision points contained in the plan?

COMMENTS:

_____

_____

_____

NSE DR REPORTS AND FORMS

The Reports are a critical mechanism for communication throughout and after the Disaster/Recovery period.

- Business Unit Key Contacts
- Summary of Critical Applications, Servers & Recovery Time Objectives (RTOs)
- Vendors & Suppliers
- Summary of Desktop & Workspace Requirements
- Other Equipment
- Critical Telephone Numbers Report

The Forms are a critical support provided to all Recovery Teams for use throughout and after the Disaster/Recovery period.

- Recovery Activities Log
- Critical Files & In-Progress Assessment
- Critical Equipment & Assessment
- Personnel Locations Control Form
- Time Sheet tracking
- Telephone Log
- Damage Control Status
- Bomb Threat Response
- Injury Status Reporting
- Receiving Room Sign-In

	Are the following key DR REPORTS used by NSE? YES or NO or DK for each
	If Yes – Describe And Identify The Distribution – Attach a SAMPLE The Reports are a critical mechanism for communication throughout and after the Disaster/Recovery period. • Business Unit Key Contacts • Summary of Critical Applications, Servers & Recovery Time Objectives (RTOs) • Vendors & Suppliers • Summary of Desktop & Workspace Requirements • Other Equipment • Critical Telephone Numbers Report

	Are the following key DR FORMS used by NSE? YES or NO or DK for each
	If Yes – Describe And Identify The Distribution – Attach a SAMPLE The Forms are a critical support provided to all Recovery Teams for use throughout and after the

	Disaster/Recovery period. • Recovery Activities Log • Critical Files & In-Progress Assessment • Critical Equipment & Assessment • Personnel Locations Control Form • Time Sheet tracking • Telephone Log • Damage Control Status • Bomb Threat Response • Injury Status Reporting • Receiving Room Sign-In

	Describe NSE DATA STORAGE related to the NSE DR Data
	Do you currently backup your servers? Do you utilize a third party for this service? Have you reviewed their BCP plan? Did this meet or exceed your requirements for service? What medium is utilized for this function? How frequently is this completed? Have you successfully tested recovering this data at an alternative location? Did this test meet or exceed your recovery objectives?

	Describe NSE DATA STORAGE related to the NSE DR Data

	Describe NSE VITAL RECORDS related to the NSE DR
	Have you inventoried your critical records? Have you secured offsite storage? What percent of records are remaining onsite? How frequently do you send offsite? Have you visited the site as part of due diligence? Have you tested that you could retrieve critical records in the time stated in service level agreement?

COMMENTS:

APPENDIX 2

2. Letter of Invitation

THE Nigerian
STOCK EXCHANGE

20th March, 2009

The Visa Office
Embassy of the Federal Republic of Nigeria
3519 International Court, NW
Washington, DC 20008
U.S.A.

Dear Sir,

LETTER OF INVITATION; MR. IRV BROWNSTEIN

This is to confirm that we have invited Mr. Irv Brownstein, Consultant for Global Information Technology, Inc. (GIT) to Nigeria to hold a series of discussions pertaining to the Nigerian Stock Exchange (NSE) Disaster Recovery Plan, which will commence on April 13, 2009 and will last approximately three (3) months.

His Passport information is as follows:

- Full name (Surname): Mr. Irv Brownstein
- Nationality: USA
- International Passport #: 212404330
- Issued By: United States Department of State
- Issued: 01/06/2005
- Expires: 01/05/2015

While on the trip, Global Information Technology, Inc. (GIT) and the U.S. Trade and Development Agency (USTDA) will be responsible for his passage and other expenses under the following appropriation:

Appropriation #: 116/71001
Activity #: 2006 11013A
Reservation #: 061113176
Grant #: GH061113176

Please accord him all the necessary assistance required to enable him to obtain his Visa.

Yours Faithfully,

PROF NDI OKEREKE-ONYIUKE, OON
DIRECTOR-GENERAL/CHIEF EXECUTIVE OFFICER

APPENDIX 3

3. NSE Network Diagrams and Resources

NSE Hardware and Resources

Per Osita (Email 8/24/09 to Mike Ike) - With respect to your request find below our high level summary response:

Software Resources:

1. We currently run on a trading platform from NASDAQ OMX called HORIZON Release h4-5-75
2. Our Operating System is IBM AIX Release 5 +
3. Our Database Software is currently ORACLE Version 10g for 8 Processors
4. Other Database Software is MS SQL Server 2003, 2005
5. Our End-user software includes Windows XP, Vista, Microsoft Office Suite
6. Anti-Virus Software includes: Mcaffee, Norton and Kaspersky
7. Stock Manager Archiving and Reporting Software

Server Hardware Resources:

8. 2 x Storage: NetApp Storage FAS 2020: 1@Production Site and 1@Backup Site
9. 2 x IBM System 570 P5 with 4 Processors: 2 @ Production Site and 1@Backup Site
10. 4 x Dual Core HP Mid Range Servers: For Web Servers, Brokers Portal, Stock Manager
11. 2 x IBM e-Servers

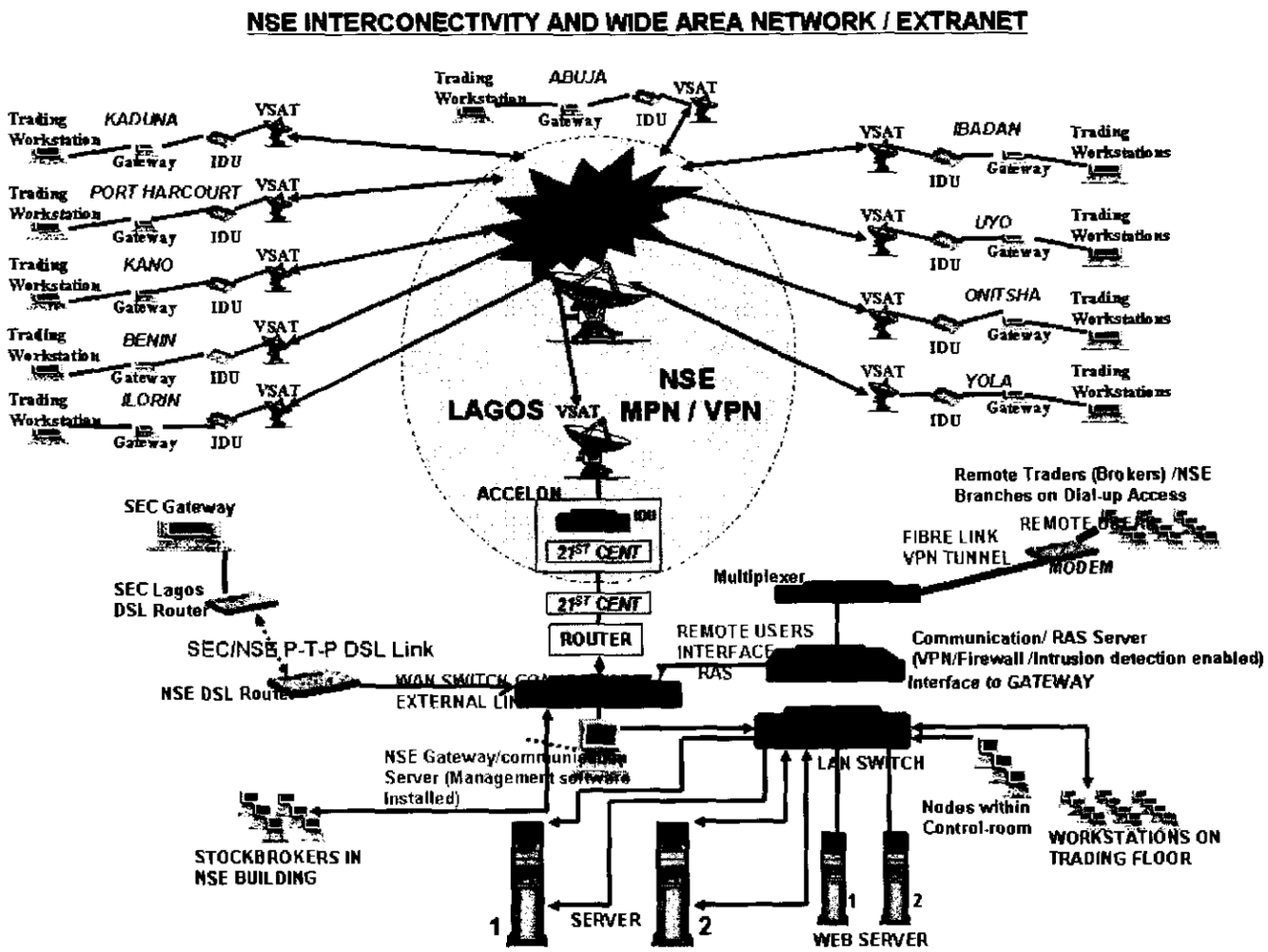
End User Hardware:

1. 100 x HP PCs runing either Windows or Vista + Network Access
2. 100 x 650VA UPS
3. 100 x 1KVA – 2KVA Power Stabilizers

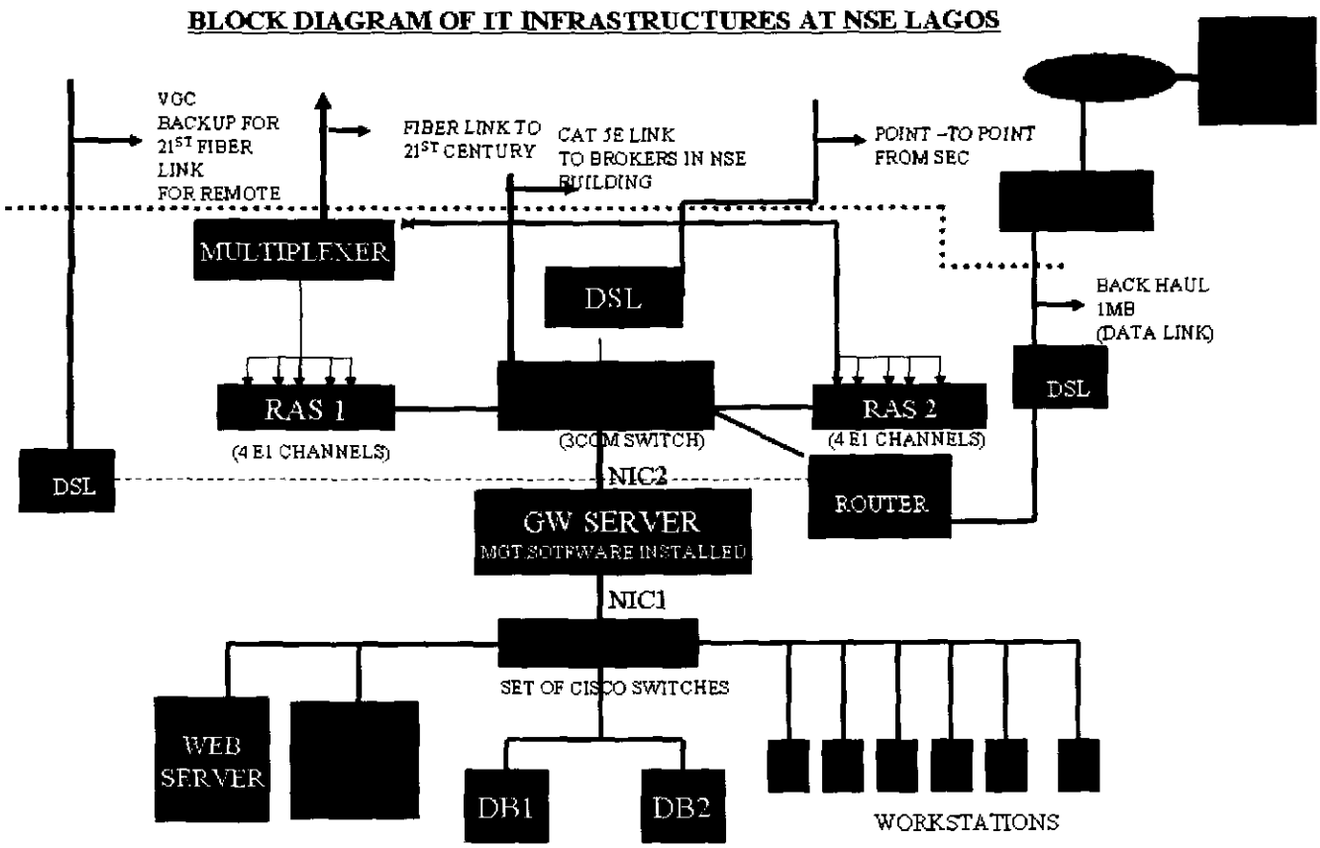
Telecoms Resources:

1. VSAT Link for Brach Connectivity to Head Quarters: Comprises In-door and Outdoor units
2. Cisco Routers and Cisco Switches for integration branch to WAN and LAN
3. Broadband Connectivity for Remote traders and regulators
4. 100Mbps Microwave link between Primary and Backup site
5. Fiber link between Trading Platform and Clearing & Settlement Platform
6. E1 linls between telco providers and NSE HQ to support broadband

NSE Interconectivity and Network



NSE IT Infrastructure



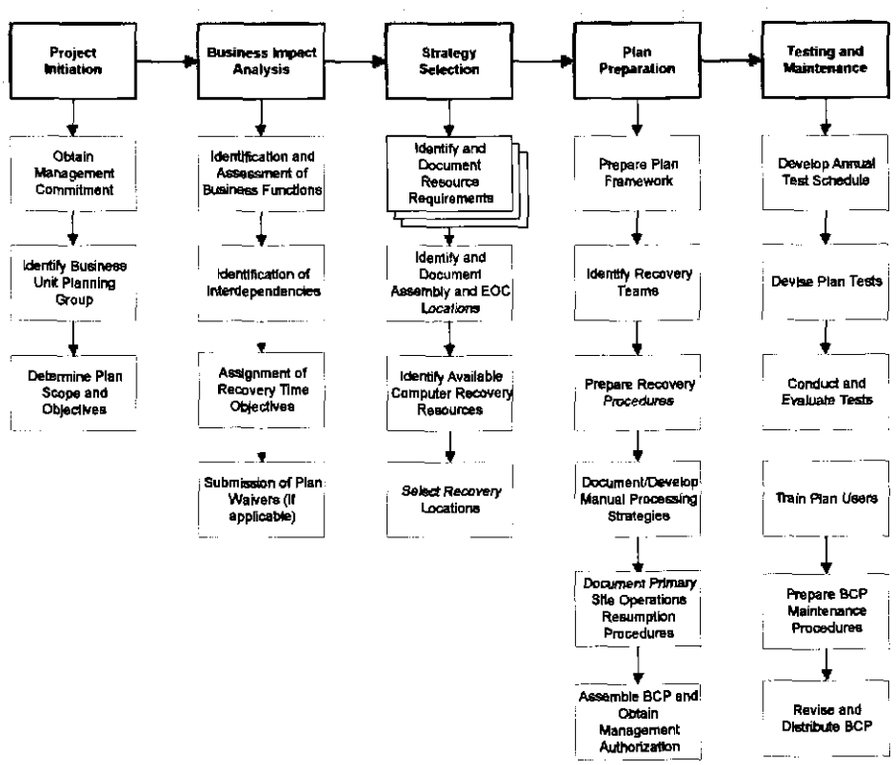
APPENDIX 4

4. NSE BCP/DRP Disaster And Contingency Plan Process

The Business Continuation Planning Process charts in the following pages provide guidance to NSE Business Continuation Planners charged with the responsibility of maintaining the DR/BC plan. The process charts depict the array of phases, steps, and tasks associated with a comprehensive plan. The five broad phases include:

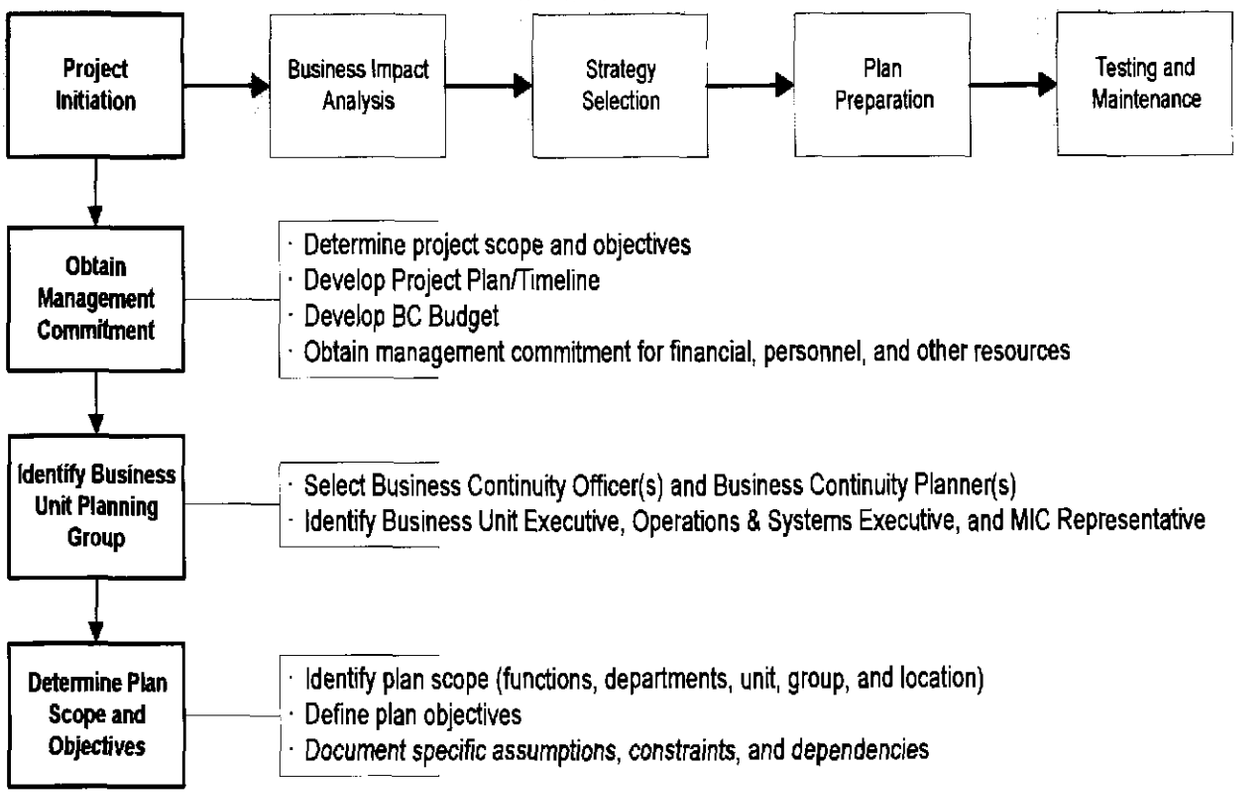
- Project Initiation;
- Business Impact Analysis;
- Strategy Selection;
- Plan Preparation; and
- Testing and Maintenance.

The Phases and Associated Steps are depicted below followed by individual the individual Steps and Tasks for each Phase.

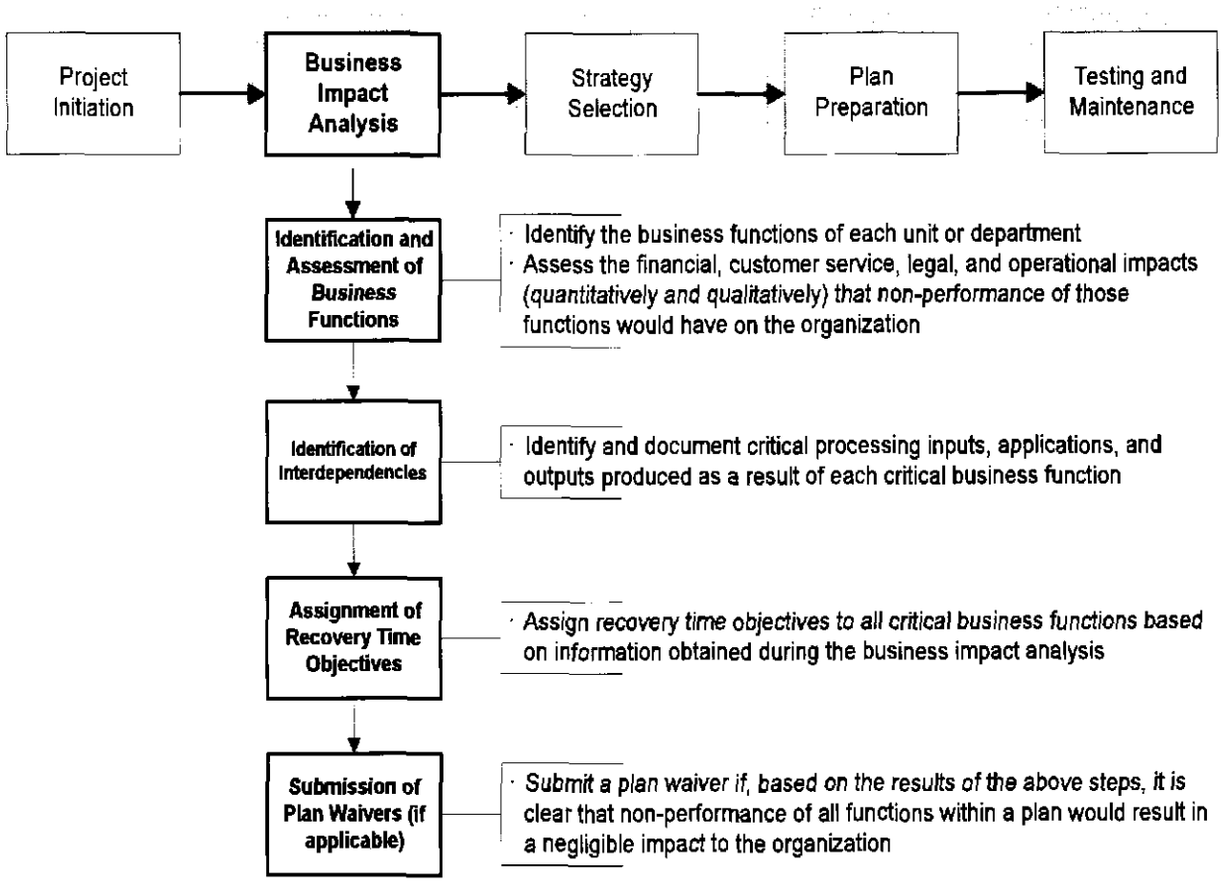


Project Initiation Phase

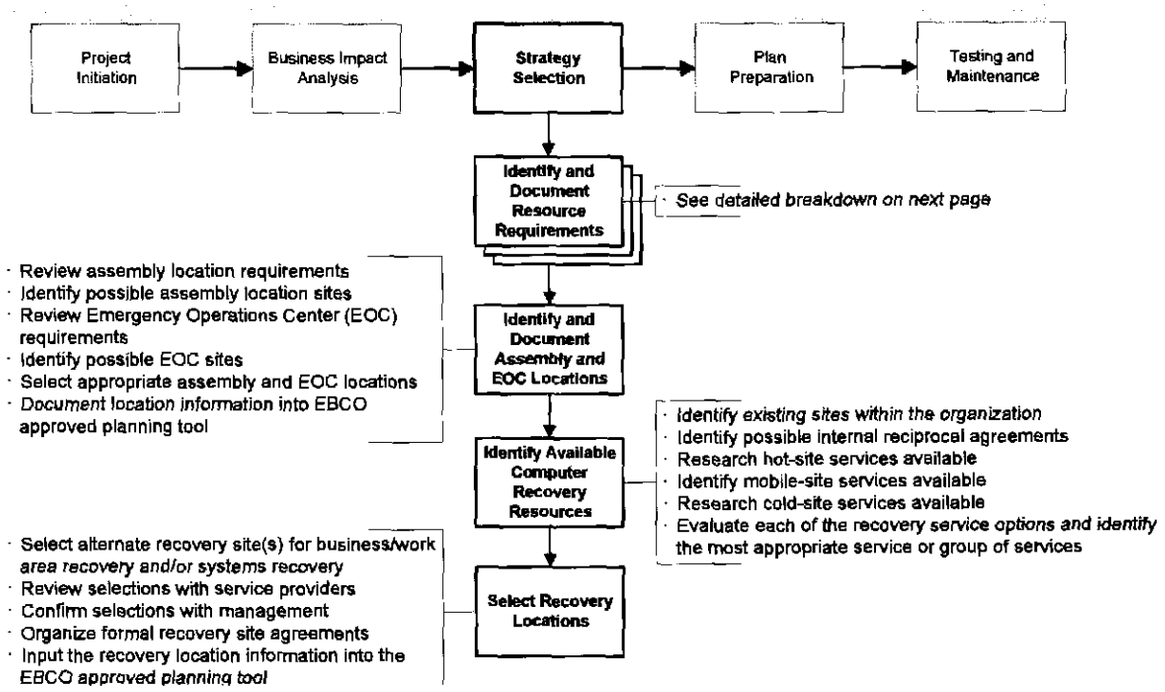
Steps and Associated Tasks



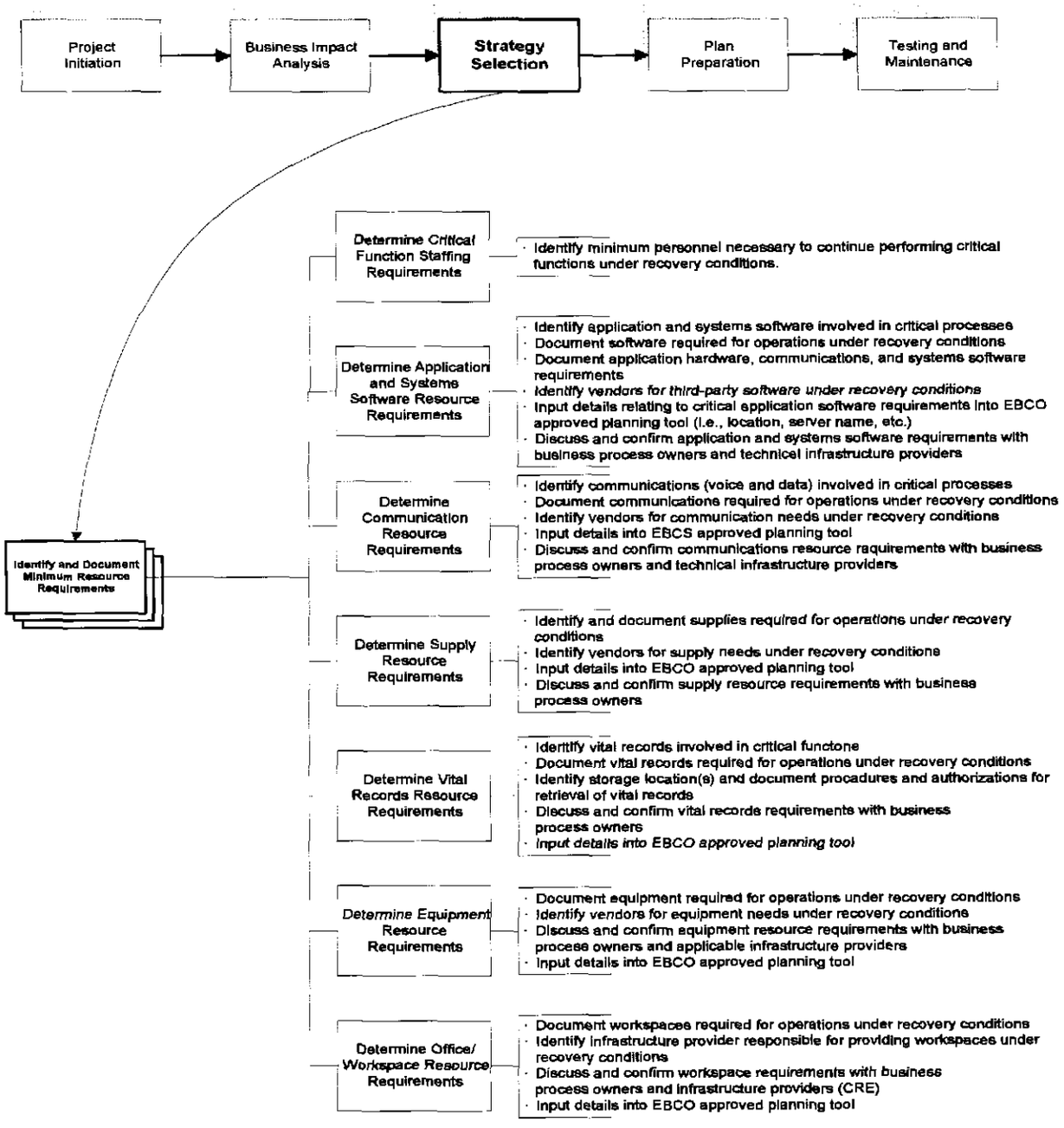
Business Impact Analysis Phase



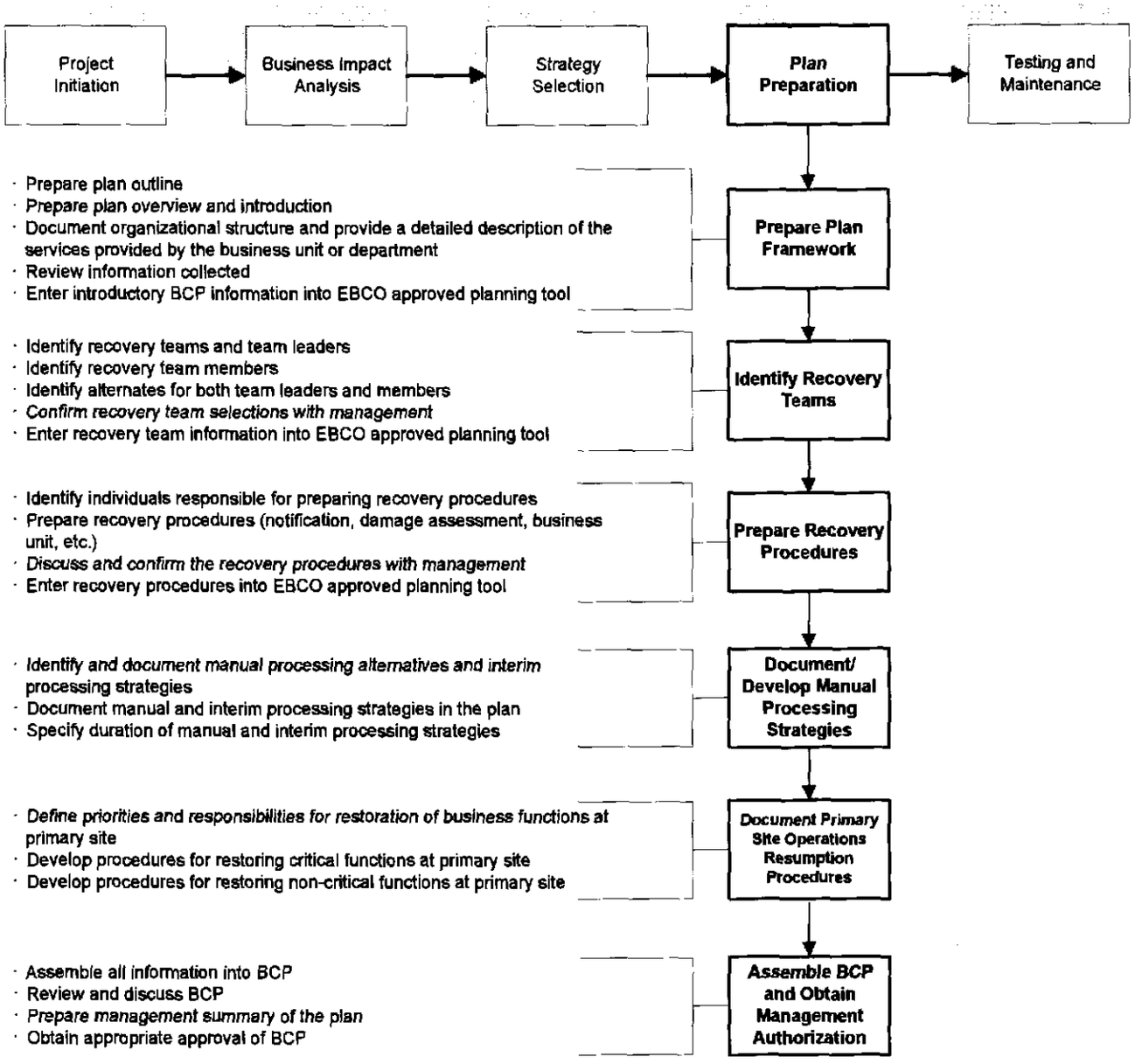
Strategy Selection Phase



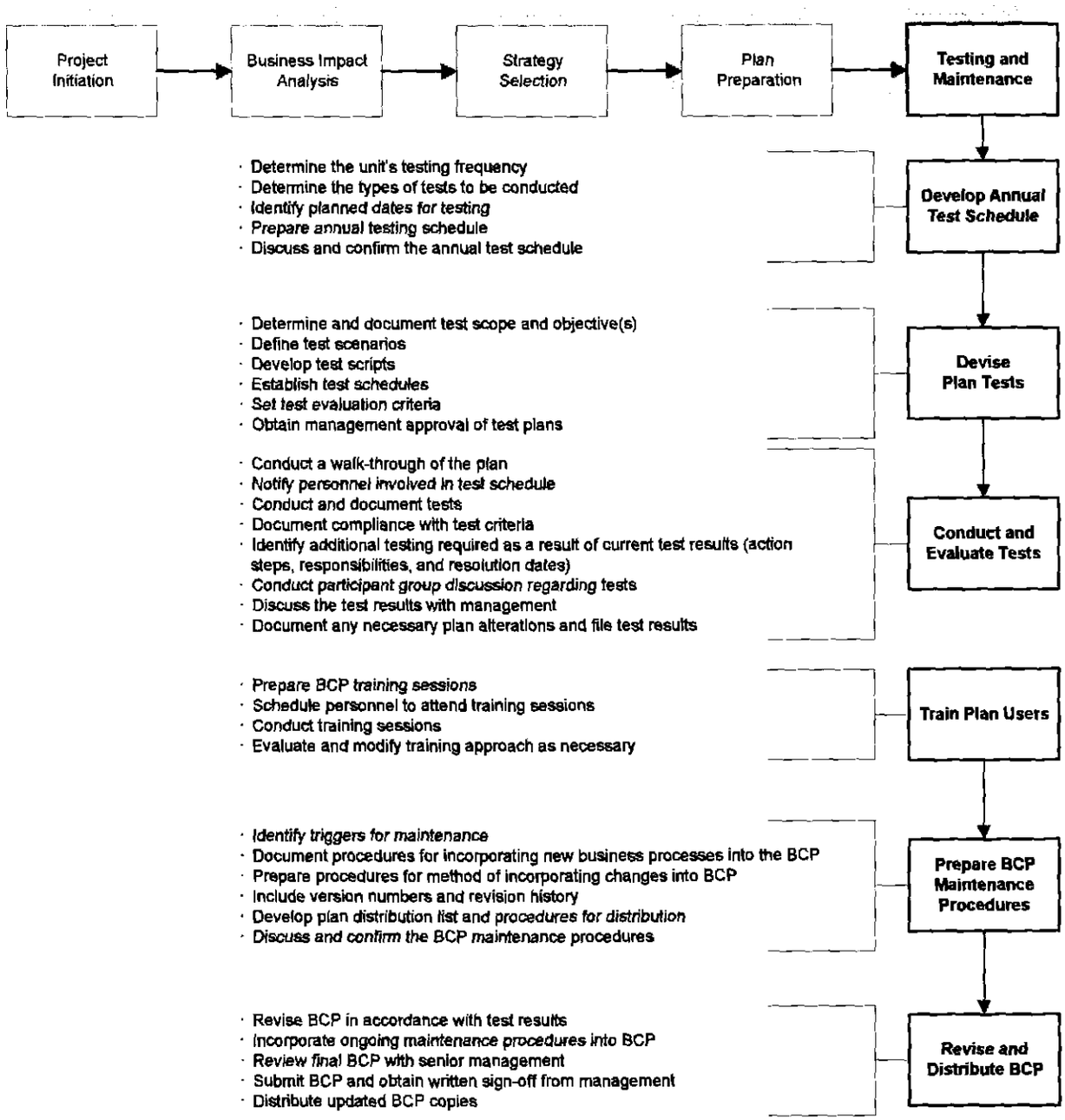
Documentation Of Minimum Resource Requirements (Detail)



Plan Preparation Phase



Testing And Maintenance Phase

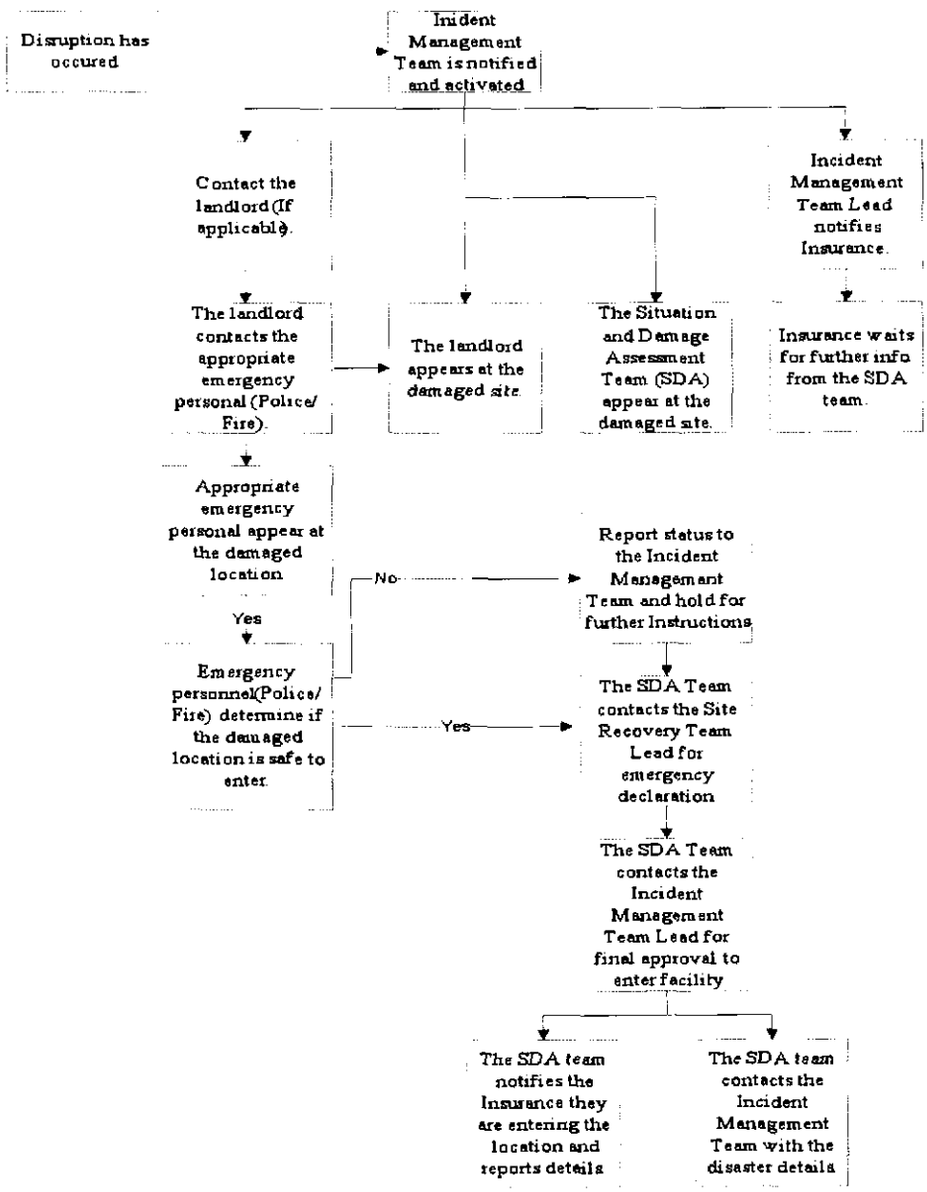


APPENDIX 5

5. Decisions Related to Failover vs. Backup

The Situation and Damage Assessment Team Leader selects appropriate personnel to travel to the damaged site to assess the damage.

Once on site, the Team follows the decision matrix shown below to determine if they should enter the damaged facility.



The Situation and Damage Assessment Team is responsible for leading damage assessment activities for all technology environments located at the affected facility.

The Team should:

- Report to the Emergency Operations Center as directed during the alert.
- Participate in the activation meeting conducted by the Incident Management Team. Acquire as much detail as possible regarding the business disruption.
- Select Situation and Damage Assessment Team personnel.
- Organize a damage assessment and restoration area near the damaged location.
- When authorization to enter the affected facility is received, brief the Incident Management Team and all assessment personnel on any restrictions or time limits, which have been imposed.
- Travel to the damaged facility to evaluate the extent of damage:
    - Structural (external & internal);
    - Critical Equipment - Utilize the Critical Equipment Status Assessment and Evaluation Form
    - Vital Information - Utilize the Critical File and Work In Process Assessment & Evaluation Form
    - Accessibility within the structure;
    - Status of telecommunications and the switch;
    - Status of cabling, terminal connections;
    - Status of all utilities;
    - Status of electrical service;
    - Status of plumbing, heating, ventilation, and air conditioning, etc.;
    - Potential environmental safety exposures.
- Assess the impact of the disaster on NSE:
    - LEVEL 1: SHORT-TERM OUTAGE (FAIL-OVER) – INTRA-DAY

A short-term outage is defined as the period of time **NSE** does not require computerized operations, or where an outage window of the same day or less would not allow adequate time to restore / utilize automated recovery operations.

- LEVEL 2: MEDIUM-TERM OUTAGE (TEMPORARY) - UP TO SIX WEEKS

  A medium-term outage is defined as the period of time that **NSE** will execute its formal disaster recovery strategy, which includes actually declaring a disaster. A disaster may either be declared company wide or only for the effected department or building. The decision to declare a disaster is based on the amount of time / expense that is required to implement the formal recovery and the anticipated impact to the **NSE** organization over this period.

- LEVEL 3: LONG-TERM OUTAGE (RELOCATION) - 6 WEEKS OR MORE

  A long-term outage is defined as the period of time that **NSE** will exceed the allowed occupancy time of its primary recovery strategy. During this phase of recovery, **NSE** will initiate a physical move of personnel and resources.

- The Situation and Damage Assessment Team Leader or Alternate Team Leader is to complete the Damage Control Status Report for use by the Incident Management Team at the Emergency Operations Center.

- Work with the Incident Management Team and contractors to develop an estimated time to reconstruct the facility:

  - Hours: _____
  - Days: _____
  - Weeks: _____
  - Months: _____

- Verify the identification of all persons entering the facility;

- Control the number of personnel permitted in the facility at any one time;
- Provide a time limit for performing impact assessment;
- Ensure that temporary security badges are distributed and worn by all vendors and visitors;
- Provide instructions for the handling of company equipment, data, files, and information to ensure that it is preserved:
    - PCs are not to be turned on;
    - Work-in-process, manuals and file information should be checked but not removed;
    - Personal items may be removed;
- Ensure that all items removed from the facility are;
- Develop and execute a salvage plan based upon the nature and extent of actual damage.

NOTE: Any person or persons responsible for removing equipment, furniture, or fixtures from the damaged site must document the move.

APPENDIX 6

6. NSE Emergency Team Composition

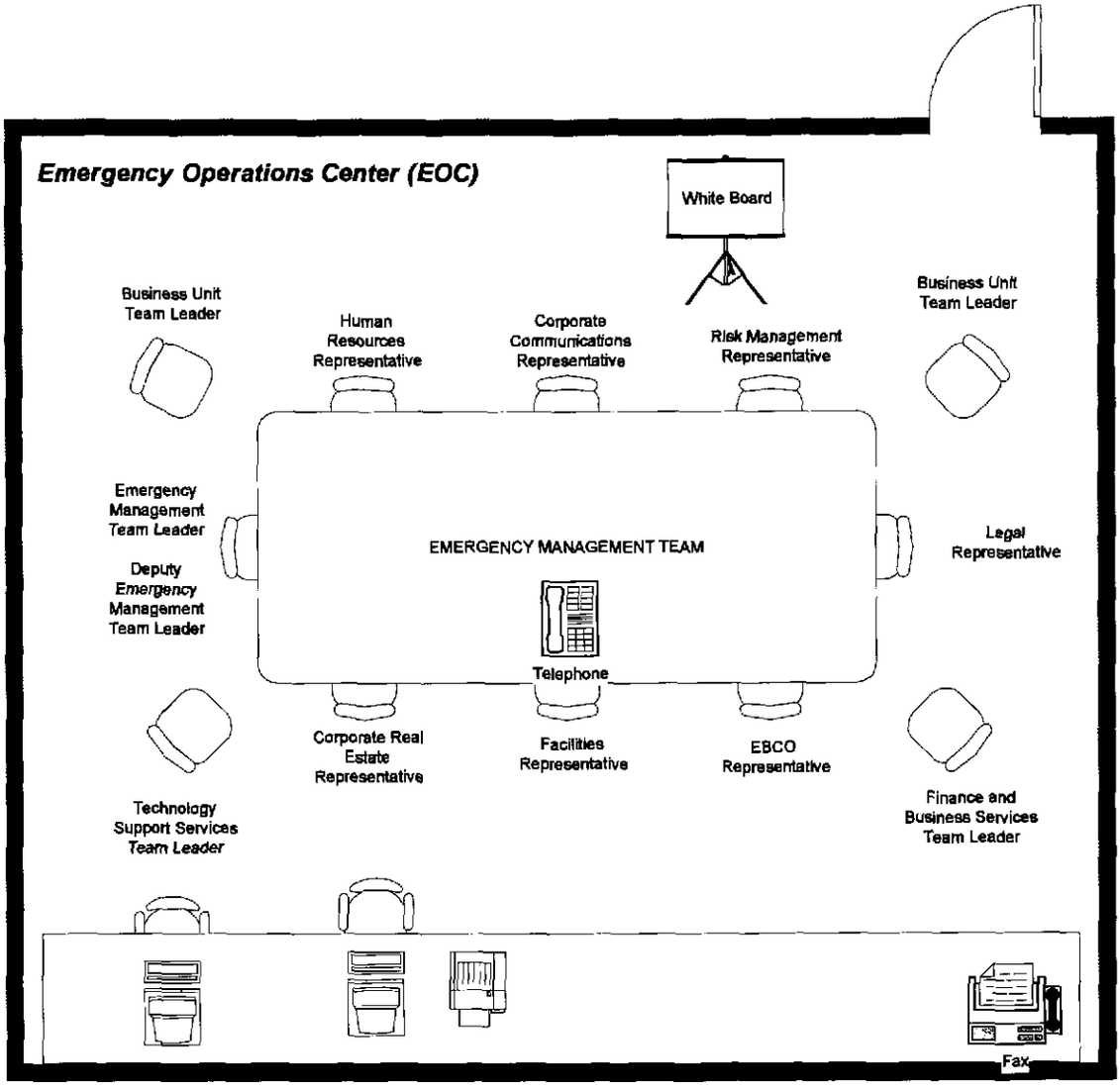
This Appendix highlights the critical formation of an Emergency Management Team and the facilities needed.

Emergency Management Team (EMT)

This diagram illustrates the members of the EMT at the Emergency Operations Center. The EMT consists of the following members (there should be one EMT per site):

1. Emergency Management Team Leader/Deputy Emergency Management Team Leader
2. Human Resources Representative
3. Corporate Communications Representative
4. Risk Management Representative
5. Corporate Real Estate Representative
6. Facilities Representative
7. Technology Support Services Team Leader
8. Legal Representative
9. Business Unit Team Leader(s)
10. EBCO Representative

NOTE: Team members should be LOCAL representatives whenever possible. Members depicted below may or may not be physically present at the EOC.


Emergency Operations Center (EOC)
White Board
Business Unit Team Leader
Human Resources Representative
Corporate Communications Representative
Risk Management Representative
Business Unit Team Leader
Emergency Management Team Leader
Deputy Emergency Management Team Leader
EMERGENCY MANAGEMENT TEAM
Legal Representative
Telephone
Corporate Real Estate Representative
Facilities Representative
EBCO Representative
Technology Support Services Team Leader
Finance and Business Services Team Leader
Fax

APPENDIX 7

7. NSE Resources

This Appendix describes the NSE resources in terms of:

- Network
  - Software
  - Server hardware
  - End User hardware
  - Telecom
- Interconnectivity
- IT Infrastructure

NSE Network Resources – Per Mr. Osita Ogbannaya

Software Resources:

12. We currently run on a trading platform from NASDAQ OMX called HORIZON Release h4-5-75
13. Our Operating System is IBM AIX Release 5 +
14. Our Database Software is currently ORACLE Version 10g for 8 Processors
15. Other Database Software is MS SQL Server 2003, 2005
16. Our End-user software includes Windows XP, Vista, Microsoft Office Suite
17. Anti-Virus Software includes: Mcaffee, Norton and Kaspersky
18. Stock Manager Archiving and Reporting Software

Server Hardware Resources:

1. 2 x Storage: NetApp Storage FAS 2020: 1@Production Site and 1@Backup Site
2. 2 x IBM System 570 P5 with 4 Processors: 2 @ Production Site and 1@Backup Site
3. 4 x Dual Core HP Mid Range Servers: For Web Servers, Brokers Portal, Stock Manager
4. 2 x IBM e-Servers

End User Hardware:

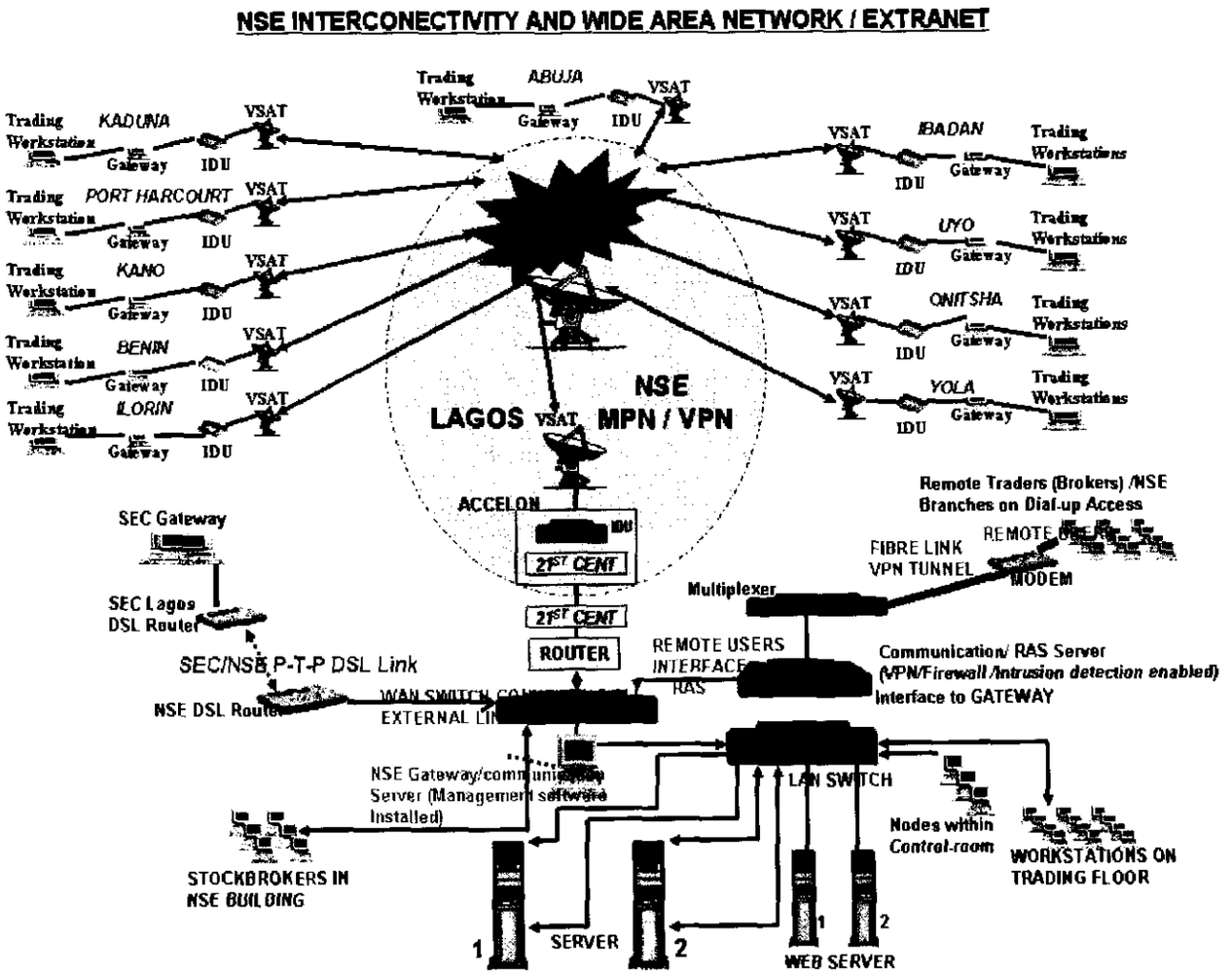
4. 100 x HP PCs runing either Windows or Vista + Network Access
5. 100 x 650VA UPS
6. 100 x 1KVA - 2KVA Power Stabilizers

Telecommunications Resources:

7. VSAT Link for Brach Connectivity to Head Quarters: Comprises In-door and Outdoor units

8. Cisco Routers and Cisco Switches for integration branch to WAN and LAN
9. Broadband Connectivity for Remote traders and regulators
10. 100Mbps Microwave link between Primary and Backup site
11. Fiber link between Trading Platform and Clearing & Settlement Platform
12. E1 linls between telco providers and NSE HQ to support broadband

NSE Interconectivity and Network



APPENDIX 8

8. NSE Implementation Plan

NOTE: See plan based Premises & Assumptions	NSE IMPLEMENTATION PLAN PHASE 1 (Tasks 4, 5, 6)		Green = In Progress & On Schedule Yellow = Potentially Behind Schedule Red = Off Schedule Blue = Complete White = Not Started & On Schedule				
PROJECT PHASE	**DELIVERABLE**	**TASK DESCRIPTION**	**RESP**	**EST EFFORT**	**DUE**	**STATUS**	**STATUS COMMENTS**
1. COMPLETE DR PLAN	PROJECT PLAN	Form NSE project team to support the DR Facility project planning, scheduling and implementation	Mr. Osita Ogbannya (OO)	5-10			
		Establish formal project structure and budget	OO	5-10			
		Develop PowerPoint presentation on project ▪ Objectives and approach ▪ Interviews ▪ Deliverables & timeframe ▪ Responsibilities	NSE Team	20-30			
		Conduct & Complete review session ▪ Answer questions ▪ Conduct Interviews	NSE Team	10-20			

NOTE: See plan based Premises & Assumptions	NSE IMPLEMENTATION PLAN PHASE 1 (Tasks 4, 5, 6)		Green = In Progress & On Schedule Yellow = Potentially Behind Schedule Red = Off Schedule Blue = Complete White = Not Started & On Schedule				
PROJECT PHASE	**DELIVERABLE**	**TASK DESCRIPTION**	**RESP**	**EST EFFORT**	**DUE**	**STATUS**	**STATUS COMMENTS**
		Gain management approval on project and launch effort	OO	1-2			
	SCORECARD	Report progress to management periodically via Scorecard (based on this plan) to management	OO / NSE Team	1-2			
2. NSE DATA COMPLETED	TEAM SELECTION	Set time frame for project launch in Lagos ▪ Identify all attendees ▪ Identify all involved & data recipients	OO / NSE Team	5-5			
		The NSE Project Team will: • Identify all relevant areas • Identify all relevant individuals • Identify all relevant functions • Identify all relevant existing materials	NSE Team	10-20			
		Complete NSE Templates using checklists, etc (See Facility Report	NSE Team	20-30			

NOTE: See plan based Premises & Assumptions	NSE IMPLEMENTATION PLAN PHASE 1 (Tasks 4, 5, 6)		Green = In Progress & On Schedule Yellow = Potentially Behind Schedule Red = Off Schedule Blue = Complete White = Not Started & On Schedule				
PROJECT PHASE	**DELIVERABLE**	**TASK DESCRIPTION**	**RESP**	**EST EFFORT**	**DUE**	**STATUS**	**STATUS COMMENTS**
		Appendices) – Call Lists; Emergency and Recovery Teams, etc.					

		The NSE Project Team collects information using a combination of instruments and templates (See Facility Report Appendices) to complete data gathering.
		
		Activities include:
		• Administer DR Procedure Templates and Forms to a wide range of stakeholders and Subject Matter Experts
		• Conduct interviews with key personnel
		• Review current documentation and records to collect for:
		  o IT Systems and Plans
		  o Mission Critical Processes
			NSE Team	40-80			

NOTE: See plan based Premises & Assumptions	NSE IMPLEMENTATION PLAN PHASE 1 (Tasks 4, 5, 6)		Green = In Progress & On Schedule Yellow = Potentially Behind Schedule Red = Off Schedule Blue = Complete White = Not Started & On Schedule				
PROJECT PHASE	**DELIVERABLE**	**TASK DESCRIPTION**	**RESP**	**EST EFFORT**	**DUE**	**STATUS**	**STATUS COMMENTS**
		○ Backup, Recovery and Security Related Operations & Business Procedures ○ Current process operations ○ NSE processing and operational constraints.					
		Customize & Finalize all procedures	NSE Team	5-5			
		Confirm Resources & Supplies	NSE Team	5-5			
		The NSE team reviews the information to gain a thorough understanding of all relevant aspects of: • *Business Continuity* • Backups available and needed • Appliance and IT Security • Physical Security	NSE Team	20-30			

NOTE: See plan based Premises & Assumptions	NSE IMPLEMENTATION PLAN PHASE 1 (Tasks 4, 5, 6)		Green = In Progress & On Schedule Yellow = Potentially Behind Schedule Red = Off Schedule Blue = Complete White = Not Started & On Schedule				
PROJECT PHASE	**DELIVERABLE**	**TASK DESCRIPTION**	**RESP**	**EST EFFORT**	**DUE**	**STATUS**	**STATUS COMMENTS**
		This analysis identifies/confirms key operations, security gaps, and/or business areas that are not properly planned in terms of recovery of operations, backup and security.					
		Identify and schedule all vendor/supplier interviews	NSE Team	5-5			
		Review Phase deliverable and project plan; modify as appropriate;	NSE Team	5-5			
3. SUPPLIER RFQ/RFP	SUPPLIER RFQ	The DR Strategic Plan outlines the needs, goals, security, and performance objectives for the future DR site.	OO	1-2			
	RFP	Create RFP template. Primary tool to be used to gather and report progress	NSE Team	5-5			

NOTE: See plan based Premises & Assumptions	NSE IMPLEMENTATION PLAN PHASE 1 (Tasks 4, 5, 6)		Green = In Progress & On Schedule Yellow = Potentially Behind Schedule Red = Off Schedule Blue = Complete White = Not Started & On Schedule				
PROJECT PHASE	**DELIVERABLE**	**TASK DESCRIPTION**	**RESP**	**EST EFFORT**	**DUE**	**STATUS**	**STATUS COMMENTS**
		Prepare RFP – identify candidates	NSE Team	5-10			
		Identify Suppliers	NSE Team	3-5			
	VENDOR LIST	Requested initial information needed to launch phase ▪ Project budget ▪ Org chart ▪ List of key participants	NSE Team	5-5			
		Conduct evaluation and select key vendor/suppliers	NSE Team	5-5			
	FINAL DR SYSTEM SPECIFICATION	Prepare and submit detailed documentation of the work performed, including the general and technical DR specifications	NSE Team	20-20			
		Review Phase deliverable and project plan; modify as appropriate;	NSE Team	5-5			

NOTE: See plan based Premises & Assumptions	NSE IMPLEMENTATION PLAN PHASE 1 (Tasks 4, 5, 6)		Green = In Progress & On Schedule Yellow = Potentially Behind Schedule Red = Off Schedule Blue = Complete White = Not Started & On Schedule				
PROJECT PHASE	**DELIVERABLE**	**TASK DESCRIPTION**	**RESP**	**EST EFFORT**	**DUE**	**STATUS**	**STATUS COMMENTS**
4. VENDOR(S) SELECTION		Review RFP plans from vendors	OO	5-10			
		Develop Scoring and evaluation criteria	NSE Team	5-10			
		Evaluate and select key vendor(s)	NSE Team	5-10			
	SELECTED VENDOR LIST	Complete and Execute Contracts with all selected vendor/suppliers	NSE Team	20-30			
		Review Phase deliverable and project plan; modify as appropriate;	NSE Team	5-5			
5. BUILD & ACQUIRE		Establish Quality Review Gates & Penalties	NSE Team	20-30			
		Build/modify Facility	NSE Team	TBD per Vendor			

NOTE: See plan based Premises & Assumptions	NSE IMPLEMENTATION PLAN PHASE 1 (Tasks 4, 5, 6)		Green = In Progress & On Schedule Yellow = Potentially Behind Schedule Red = Off Schedule Blue = Complete White = Not Started & On Schedule				
PROJECT PHASE	**DELIVERABLE**	**TASK DESCRIPTION**	**RESP**	**EST EFFORT**	**DUE**	**STATUS**	**STATUS COMMENTS**
	DR FACILITY	Review and Approve	NSE Team	10-20			
		Review Phase deliverable and project plan; modify as appropriate;	NSE Team	5-5			
6. LOAD & TEST		Develop Test Plans	NSE Team	20-30			
		Confirm Alerts & Performance Reporting Factors, time frames and Distribution	NSE Team	20-30			
		Load Systems & Materials	NSE Team	30-50			
	DR TEST BED	Implement Failure Test	NSE Team	20-30			
		Review Phase deliverable and project plan; modify as appropriate;	NSE Team	5-5			

NOTE: See plan based Premises & Assumptions	NSE IMPLEMENTATION PLAN PHASE 1 (Tasks 4, 5, 6)		Green = In Progress & On Schedule Yellow = Potentially Behind Schedule Red = Off Schedule Blue = Complete White = Not Started & On Schedule				
PROJECT PHASE	**DELIVERABLE**	**TASK DESCRIPTION**	**RESP**	**EST EFFORT**	**DUE**	**STATUS**	**STATUS COMMENTS**
7. MANAGEMENT REVIEW	PRESENTATION	Collect all results and data from each work stream	NSE Team	10-20			
		Develop draft presentation - the team prepares the Presentation based on the analysis from plan phases 1 – 6 to provide: ▪ a summary of the efforts to date ▪ CSCS backup and recovery initiatives, ▪ mission-critical trading operations, and ▪ business processes at the NSE for business continuity and disaster recovery. The Team also details the performance results of the vendor(s) selected	NSE Team	20-30			

NOTE: See plan based Premises & Assumptions	NSE IMPLEMENTATION PLAN PHASE 1 (Tasks 4, 5, 6)		Green = In Progress & On Schedule Yellow = Potentially Behind Schedule Red = Off Schedule Blue = Complete White = Not Started & On Schedule				
PROJECT PHASE	**DELIVERABLE**	**TASK DESCRIPTION**	**RESP**	**EST EFFORT**	**DUE**	**STATUS**	**STATUS COMMENTS**
		Conduct internal review and Modify Presentation as necessary	OO / NSE Team	10-15			
		Conduct Presentation This checkpoint helps to determine any further efforts and key business and operational areas and/or functions targeted for disaster recovery.	OO / NSE Team	5-10			
	LESSONS LEARNED	Conduct Lessons Learned	NSE Team	10-15			
		Prepare Feedback on results and Lessons Learned for Management Review and Action	OO / NSE Team	5-5			
8. FIRE DRILLS		Conduct Periodic Tests	NSE Team	20-30			

NOTE: See plan based Premises & Assumptions	NSE IMPLEMENTATION PLAN PHASE 1 (Tasks 4, 5, 6)		Green = In Progress & On Schedule Yellow = Potentially Behind Schedule Red = Off Schedule Blue = Complete White = Not Started & On Schedule				
PROJECT PHASE	**DELIVERABLE**	**TASK DESCRIPTION**	**RESP**	**EST EFFORT**	**DUE**	**STATUS**	**STATUS COMMENTS**
	FIRE DRILL REPORT	Ensure DR and Facility are current, correct and perform as required and specified	NSE Team	10-20			
		Prepare Feedback on results and Lessons Learned for Management Review and Action	OO / NSE Team	5-5			
9. END IMPLEMENTATION PLAN							

APPENDIX 9

9. NSE BCP Standards

This Appendix describes twenty-four (24) standards grouped into five (5) key groups used by NSE to manage planning and execution of Business Continuity and Disaster Recovery. The groups of standards are:

- BC/DR Planning Related
- BC/DR Recovery and Restoration Factors Related
- BC/DR Testing Related
- BC/DR Quality and Control Related
- BC/DR Staff Related.

BC/DR Planning Related

Commitment Of Management Resources

Every business group must develop business continuation plans for all critical business functions. Each business group must identify the appropriate business continuation individuals responsible for business continuation planning among each of the organizational units within the business group. These include:

- Business Continuation Officer(s),
- Coordinator(s), and
- Planner(s))

Plan Authorization

All plans must be reviewed and approved by the group's Business Continuation Officer, appropriate Business Unit Management, Operations & Systems Executive, and unit MIC Officer who are responsible for validating critical business functions and their related recovery time objectives as well as other plan components necessary to resume business in a timely manner in the event of a disaster.

Assessment Of Business Functions

Business units must perform a business impact analysis to evaluate the financial and non-financial impacts of a worst-case disaster scenario on each particular function.

Identification Of Interdependencies

Business units must address work flow interdependencies between their own function's processes and other business units and/or external sources.

Contingency Resource Requirements
The business continuation plan must identify all computing, workspace, vital records, and other resources required to support the unit's critical business functions. The plan must specify the minimum resources within specified recovery time objectives.

Plan Scope And Objectives
All business continuation plans must clearly define plan scope and objectives. In addition, plans must develop recovery procedures to address the following scenarios:

1. Building and/or work area is inaccessible (computer environment is available);
2. Computer environment is unavailable (work area is accessible);
3. Loss of key interdependency (internal and/or external);
4. Communications failure; and
5. Specific geographic vulnerability (high exposure to earthquakes, flooding, hurricanes, etc.).

Manual And Interim Processing Strategies
Plans must include interim and manual processing strategies where those procedures currently exist or where they may prove useful or necessary to ensure the continuation of critical business operations. Strategies must include information security provisions.

Plan Maintenance
The business continuation plan must be reviewed quarterly to ensure that all required updates have been performed. Document control procedures must be implemented in order to protect the integrity of the plan.

BC/DR Recovery and Restoration Factors Related

Assignment Of Recovery Time Objectives

Business units must assign a recovery time objective to each business function based on the results of the BIA.

The following intervals must be used for classification of both critical functions and resource requirements:

RECOVERY NEED	INTERVAL
Immediate	1
Within 24 hours	2
Within 72 hours	3
Within 1 week	4
Within 2 weeks	5
Within 30 days	6
Beyond 30 days[1]	7

Recovery Teams
Recovery teams, team members and their alternates must be identified.

Recovery Procedures
Disaster declaration, evacuation, damage assessment, emergency response, and off-site storage and retrieval procedures must be documented in the plan; all procedures must provide sufficient detail. Business units must identify specific prioritized activities for the recovery of all critical business functions. Normal security provisions and controls must be maintained for recovery procedures.

Site Restoration Procedures
The plan must address procedures for restoring business functions to the primary site.

Alternate Site Recovery Solution
Every organizational unit must be prepared to relocate critical business functions to an alternate site and resume operations. Efforts will be focused on selecting an internal, cost-effective recovery solution. In the event that external vendor solutions need to be considered, the business unit must prepare and submit a cost-benefit analysis to their business unit management and the EBCO. Alternate site agreements, whether internal or external, must be included in the plan document.

BC/DR Testing Related

Testing The Plans
Business continuation plan test exercises must be conducted to demonstrate the ability of the business unit to recover its critical business functions within specified recovery time objectives. Business units must comply with Enterprise information security standards when performing test exercises. All business units must develop a reasonable test strategy and schedule.

Minimum Levels Of Testing Required
Business units must test their business continuation plans consistent with the frequencies derived from the business unit's critical business function recovery time objectives.

Following are minimum testing frequencies by Recovery Time Objective. See Standard Testing the Plans, for descriptions of the three levels of testing.

TEST LEVELS VS. RECOVERY TIME OBJECTIVES	STRUCTURED WALK-THROUGH (TABLE-TOP EXERCISE)	COMPONENT TESTING	INTEGRATED SIMULATION (FULL OPERATIONS TEST)
(Critical) Interval 1 - Immediately	Semi-Annual	Annual	Annual
Interval 2 - Within 24 hours	Semi-Annual	Annual	Annual
Interval 3 - Within 72 hours	Semi-Annual	Annual	Annual
(Important) Interval 4 - Within 1 week	Annual	18 months	18 months
Interval 5 - Within 2 weeks	Annual	18 months	18 months
Interval 6 - Within 30 days	Annual	18 months	18 months
(Non-critical) Interval 7 - Beyond 30 days	Optional	Optional	Optional

Evaluation And Documentation Of Test Results

Test results must be evaluated and documented subsequent to test completion. The business unit needs to assess the results against predefined test objectives and communicate the evaluation to the business unit executives. The Business Continuation Plan must be revised in view of the test results.

BC/DR Quality and Control Related

Waiving Of Firm Policies
In a disaster situation, it may be necessary to waive firm policies in order to ensure the successful recovery of critical business operations. Emergency delegation of authority guidelines (DAGs) must be developed for each business group.

Plan Waiver
In very limited circumstances and based on the results of a completed, a Business Continuation Officer may request a plan waiver on behalf of a particular business unit. The written request,

communicated to the EBCO, must be approved by the business unit's executives, the business group's Management Internal Control (MIC) representative, and Internal Audit.

Vital Records
Vital records must be identified, protected from destruction, and copies stored off-site where appropriate. Procedures must be developed to ensure that the off-site records remain current.

Assembly And EOC Locations
Primary and alternate assembly and Emergency Operations Center (EOC) locations must be identified and documented in the plan.

Documentation And Plan Format Requirements
Business Continuation Plans for all organizational units are to be documented consistent with these Enterprise standards. All business continuation plans must contain certain key elements. Confidential and sensitive information (i.e., passwords) in plans that are stored electronically must be encrypted.

BC/DR Staff Related

Organization Chart
Organization charts and a description of the services normally provided by each organizational unit must be included in the plan document.

Third Party Vendor Certification
Business units need to verify that critical third party vendors meet specific business continuation planning requirements.

Staff Awareness
Procedures must be established for informing and keeping staff current on business continuation planning and individual responsibilities. Plan content and implementation must be fully understood by all staff.

APPENDIX 10

10. NSE BCP Plan, Emergency Actions & Procedures

This Appendix contains extensive information and detailed procedures for Emergency Response, Recovery, and Restoration operations for NSE departments in the event of a disruption including:

- Procedures that allow NSE departments to respond appropriately to a business disruption
- The teams that complete the specific activities necessary for emergency response and recovery
- The critical business functions that need to continue after a disaster
- The logistics of recovering critical business functions
- The procedures for releases of information to employees and the general public
- Ensure the safety of employees and visitors of NSE departments.

Procedure Overview

Policy Statement

It is the policy of the NSE that all business groups, subsidiaries, and corporate departments are required to have business continuation plans in place that address business outages such as disaster preparedness, response, recovery and restoration. Plans should be developed and maintained based on ongoing risk management and business impact analysis reviews. Plans must be reviewed and tested according to Enterprise Business Continuation standard timelines.

A disaster is a disruption of business operations for an unacceptable period of time. The purpose of the Business Continuation Plan is to provide NSE departments with the means to accomplish this policy in an effective and organized way.

This document contains information, procedures and reference material for Emergency, Recovery, and Restoration operations for NSE departments in the event of a disruption affecting the NSE facility. The objectives of this written document are:

- To define procedures that will allow NSE departments to respond appropriately to a business disruption
- To identify key individuals who will manage the process of recovering the business after a disaster
- To identify the teams that will complete the specific activities necessary for emergency response and recovery
- To specify the critical business functions that need to continue after a disaster

- To outline the logistics of recovering critical business functions
- To catalog interdependencies and resources that can assist in this process
- To establish procedures for releases of information to employees and the general public
- To ensure the safety of employees and visitors of NSE departments

This document is evolutionary in nature and is maintained by the NSE departments Business Continuation Planner. It is imperative that all involved parties in NSE departments keep the Business Continuation Planner advised of all:

1. Changes to internal policies, procedures, and operations which might impact the content of the Business Continuation Plan

2. Changes in personnel which have an impact on the assignments of responsibilities for the tasks within this plan

Scope of Procedures

This plan focuses on the minimum acceptable procedures and configuration necessary for continued support of mission critical functions and systems that NSE departments supports.

This plan is designed for business disruptions resulting from localized events through regionalized disasters. Catastrophic events that are beyond this level of severity (e.g., nuclear war, plague, etc.) are extremely improbable and are not considered in this plan.

The complete list of possible disasters is too numerous to list. This plan deals with the results of the event regardless of its cause. The results can be categorized into three general scenarios.

1. **Localized Disaster** - Such as a fire that destroys all or part of the building. This scenario will require partial or even total relocation of business operations to a recovery site. In addition the building may require extensive restoration before normal operations can resume.
2. **Denial of Access** - The building and contents are intact, but access is cut off. This can be caused by a nearby chemical spill, lack of water or power, or an occurrence of workplace violence. Generally, the building and its contents are not severely damaged and therefore, little if any restoration is required.
3. **Regional Disaster** - Any disaster that affects the Lagos area. The most likely will be a power outage that will affect all the NSE properties in the area.

The structure of the plan has been designed to allow complete or partial mobilization of resources. The level of response can be scaled up or down to match the severity of the actual

event. This approach ensures that critical business functions continue to operate without incurring unnecessary expenses.

The plan is specific to NSE departments, and does not address the recovery of other the NSE operations that may reside in or close to the NSE building.

Assumptions

This plan assumes one of the three scenarios listed above. Assumptions that hold during all three scenarios are:

- The plan is kept up to date, and all participants are familiar with their respective roles and responsibilities, and that sufficient number of staff are available to accomplish the goal and objectives of the plan
- Vital records are intact, retrievable and may be accessed
- External dependencies such as the NSE's processing facilities will either be unaffected or recovered.
- Project Managers for Mission Critical systems have reviewed the relevant plans developed by Business Partners and the respective the NSE's production operations. Where plans exist, the plan values are consistent with expectations and coordinated with the values in the NSE departments plan. Where no plan exists, the Project Manager has formally communicated his/her concern.
- Mission Critical systems plan values will be kept synchronized with Business Partner and the NSE's plans
- All necessary technology dependencies such as mainframe, servers, workstations, applications, communications, and databases are functional or have been recovered
- Alternate locations designated for recovery support will themselves be available
- Normal operating procedures and/or level of service may be altered to ensure recovery of critical functions
- The recovery organization of management and staff may not reflect that which is present during normal operations

Business Impact Analysis

A detailed Business Impact Analysis was conducted to identify the probable effects to the business in the event of a disruption at NSE departments.

The primary responsibility of NSE departments is the support of business and Trading systems within the Exchange. Several of these systems are critical to gaining revenue, supporting the financial infrastructure and compensating associates and agents. Therefore, a business disruption at NSE departments could cause a degradation of, or inability to meet obligations to internal or external parties.

Critical Business Functions

A critical business function is an activity or service that if lost, would adversely affect the NSE's ability to function or carry out its mission objectives. An impacted critical business function would cause the company or its customers to suffer significant financial or non-financial (including reputation) losses.

The critical business functions of NSE departments are summarized in the table below. For each function, a recovery time objective was assigned as a result of the business impact analysis conducted prior to the creation of this plan. The recovery time objective is the maximum amount of time that the function can be suspended before causing a severe impact to the unit's mission or responsibilities.

NSE DEPARTMENTS

CRITICAL BUSINESS SYSTEMS/FUNCTIONS	RECOVERY TIME OBJECTIVE

Note: All recovery time objectives, other than immediate, reflect business days or weeks.

Recovery Strategies

Three basic strategies have been evaluated for applicability to affect a recovery of each component of NSE department's functionality.

1. The first strategy ("Transfer of Work") is to transfer the work handled by NSE departments to other locations where it will be processed by external staff and resources.

2. The second strategy ("In House Recovery") is to recover functionality using the staff and resources from NSE departments at an alternate work location.
3. The third strategy ("At Home") is to recover functionality using the staff and resources from NSE departments at home locations utilizing remote accessibility.

Although each strategy has its advantages and disadvantages as outlined below, NSE departments generally will use options II and III during an interruption.

1. TRANSFER OF WORK	
Advantages	***Disadvantages***
• Can be done relatively quickly • Works regardless of damage severity • Requires little initial set up cost	• Places burden on recipient business unit • Lack of staff familiarity may impact work quality and customer satisfaction
2. IN HOUSE RECOVERY	
Advantages	***Disadvantages***
• Minimizes impact on other business units • Continuity of staff has positive effect on quality and job performance • Degree of resources deployed can be scaled to match severity of event • Improved morale and confidence results from employees recognition of their role in planning and plan implementation	• Typically takes more time to implement • Recovery may not be practical with some severe disasters which affect availability of staff and/or recovery locations • Cost of required resources and strategy implementation typically require a greater investment of capital • Planning for staff relocation, as well as establishment of infrastructure and support at time of disaster, requires extensive and detailed planning
3. AT HOME	
Advantages	***Disadvantages***
• Can be done relatively quickly • Works regardless of damage severity • Requires little initial set up cost	• Lack of staff ability to interact may impact work quality • Lack of equipment and remote accounts may limit response

Phases Of Response

A disaster response consists of three distinct phases: Emergency; Recovery; and Restoration. Each has its own set of objectives. The duration of each phase will depend on the nature of the event and its effect on NSE departments' critical business functions.

1. **Emergency Response** - These are the immediate actions, which are taken during the initial stages of the event. Their purpose is to protect life and property as well as to notify all involved parties. Once this is accomplished the priority shifts to mitigation of damage and preservation of business operations. A determination of whether to declare a disaster will be made based on detailed evaluations of the event's impact on Enterprise Solution's critical business functions.

2. **Recovery Operations** - These actions begin as soon as a disaster has been declared. The objective of Recovery is the continuation of NSE departments' critical business functions. This phase continues until restoration is complete and operations return to normal.

3. **Restoration Operations** - This phase includes the tasks required to reestablish the business to the level it was prior to the disaster. Restoration runs concurrently with Recovery Operations.

Recovery Organization

The recovery organization for NSE departments combines management infrastructure and critical business system functions. Wherever possible, an effort has been made to staff teams with personnel familiar with the tasks and duties to be performed. In some cases, individual areas that function autonomously under normal conditions have been merged to maximize the efficiency and effectiveness of the recovery.

The first team to respond to an event will be the Emergency Management Team, which will be responsible for evaluating the situation and initiating the Business Continuation Plan. As the plan is activated, team members will mobilize and begin recovery operations. Information on specific functional area structure, objectives, procedures and resources can be found in Section Three.

Roles And Responsibilities

Note: See the Implementation Plan section

The list outlines the key responsibilities as they pertain to business continuation plan development, maintenance, and implementation. W

hile some of the roles are external to NSE departments, nevertheless they are essential to the effectiveness of its plan.

Distribution Policy

The business continuation plan document contains confidential information that should only be viewed by those individuals that are involved in its creation, maintenance, implementation, or validation. Distribution of the plan in its entirety is generally limited to the site Business Continuation Planner, senior management, members of the Enterprise Business Continuation Office, and authorized internal and external audit/compliance parties. Various sections of the plan may be distributed to individuals who are involved in particular aspects of business continuation but may not have a need to view the complete document.

While access to the document itself is limited to designated individuals, the knowledge of its existence and objectives should be widely disseminated throughout the entire organization. This will add to employee confidence and moral, as well as increase the likelihood for a successful recovery in the event of an actual disruption.

Emergency Mobilization

This section covers the process by which the business continuation plan is activated. As explained earlier, a business disruption has three distinct phases: Emergency, Recovery, and Restoration. The emergency phase is considered the period from the onset of the business disruption, or emergency situation, through the mobilization of recovery resources. It should be noted that not all disruptions are emergencies, and not all emergencies will be declared disasters. A hasty decision to declare a disaster can be more disruptive than the event itself. A timely and appropriate response however is necessary to protect the safety of employees and reduce the risk to property.

Emergency Operations Center

The emergency operations center (EOC) is the focal point of communication and coordination for resources during a business disruption. At this location, the emergency management team (EMT) convenes to analyze information on the disruption and decide how NSE departments will respond to it. The EOC itself is not a recovery location. However, it may be co-located with a recovery site for one or more of the critical business functions.

The EOC functions as the command and control center for the recovery and restoration effort. It is here that senior management of NSE departments can monitor the recovery and restoration process. The actual location of the EOC must be unaffected by the events that have caused the business disruption and must be assessable by the majority, if not all, of the EMT members. As a minimum, communication into and out of the EOC must be adequate to coordinate all aspects of initial emergency response, recovery, and restoration, and the occupants must not be in physical danger.

Two sites have been selected as possible EOC locations. The preferred site has been designated as the primary EOC and is located at:

TBD per NSE

The secondary EOC is located at:

TBD per NSE

The EMT will convene at the primary EOC if conditions allow. In the event that the primary EOC is not available, or the secondary site is deemed preferable by NSE department's executive, the secondary site will be selected.

Some disruptions may only affect a portion of the primary facility. In this event the EMT has the authority to select an alternate EOC that may reside in an unaffected area of the building. Other alternate locations may be selected as well, such as local hotels, businesses, or possible even an associate's home. Before an alternate site is chosen however, the communication and connectivity capabilities of that location must be considered. Regardless of the selected site for the EOC, the exact location must be communicated to all members of the EMT upon mobilization, and to all external parties upon notification when necessary.

Emergency Management Team

The EMT is responsible for coordinating the response to the emergency or disruption as well as the recovery and restoration effort. The structure of the EMT is designed to provide representation from the business areas, and any other area, which impacts the critical business functions. The members of the EMT will advise the team leader, who is also the NSE department's executive. While the team leader has sole responsibility for disaster declaration, this decision will be made based on information provided by the team members.

The EMT is also responsible for communication with other the NSE organizations, as well as non-NSE parties not specifically addressed by individual critical function team plans.

Emergency Operation Center Preparation

In order to facilitate effective operations at the EOC, various material resources must be pre-positioned at the site or readily obtainable at the time of EMT mobilization. These resources are categorized as essential or recommended to enhance the EOC response.

Essential

- Current version of the Business Continuation Plan
- Any additional contact information that may not be contained in the current version of the Plan
- Telephone
- Fax
- Paper, Pens, and Pencils

Additional Recommended Items

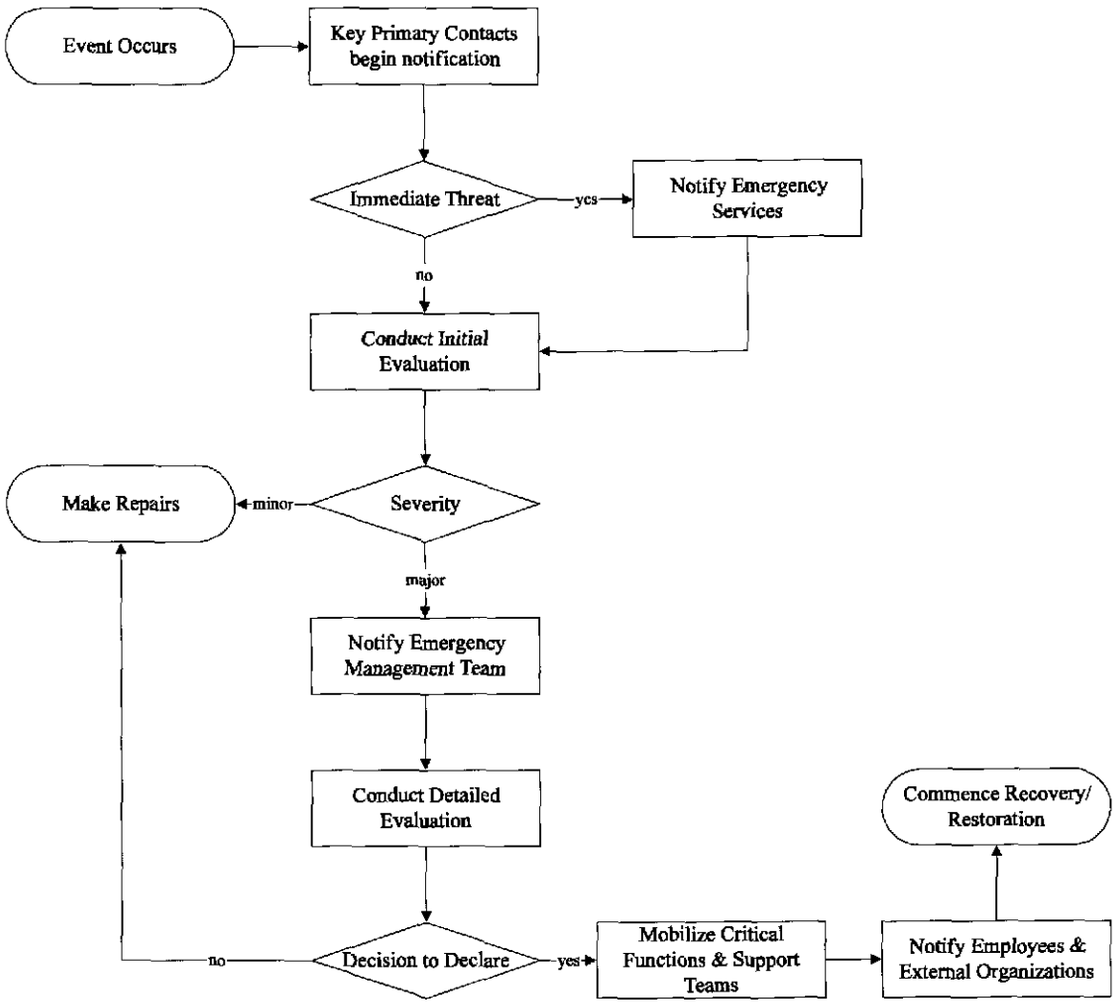
- Cell Phones w/ Charged Batteries (Issued to EMT Members Prior to Disaster)
- Alpha Numeric Pagers (Issued to EMT Members Prior to Disaster)
- Chargers for Cell Phone Batteries
- PC with e-mail Capability and Standard Microsoft Office
- Modem Ready Line for Remote Connectivity
- Printer
- Walkie-Talkie
- Portable Radio/TV
- Satellite Telephone
- Flashlights
- Hard-hats and Protective Clothing
- Additional Office Supplies

Some of these items will require periodic maintenance.

A schedule for this should be incorporated in the normal business continuation plan maintenance schedule.

Emergency Procedures

The chart below outlines the steps taken during notification and mobilization. The procedures that follow indicate who is responsible for the specific actions.


Event Occurs
Key Primary Contacts begin notification
Immediate Threat
yes
Notify Emergency Services
no
Conduct Initial Evaluation
Make Repairs
minor
Severity
major
Notify Emergency Management Team
Conduct Detailed Evaluation
Commence Recovery/ Restoration
no
Decision to Declare
yes
Mobilize Critical Functions & Support Teams
Notify Employees & External Organizations

	NSE PROCEDURES	WHO
1.	**ACTIVATE EMERGENCY PROCEDURES/NOTIFY SITE EXECUTIVE** Upon discovery of an emergency, immediately activate emergency procedures in accordance with the property manager's policy for life safety and damage mitigation. The Primary Contacts will notify NSE departments Executive, or alternate, and provide the status of the facility/event.	
2.	**EVALUATE THE SITUATION** The primary contacts will provide NSE departments Executive or alternate with information on the incident/threat, including estimated duration of the disruption. Based on this initial information, NSE departments Executive will determine if the Emergency Operations Center should be mobilized and the business continuation plan activated.	
3.	**DETERMINE EMERGENCY OPERATIONS CENTER LOCATION** The incident will dictate which Emergency Operations Center (EOC) location will be selected for activation. Generally, if the incident has affected only the NSE departments building, the primary EOC location will be chosen. If the incident is more wide spread, and affects the secondary EOC location will be selected. In the event that the disruption does not affect the entire facility, a conference room or similar space may be used as an alternate EOC.	
4 a.	**ACTIVATE EMERGENCY OPERATIONS CENTER (PRIMARY)** Contact the Training Center and inform them that an emergency situation exists and requires the activation of their training room. Ensure that any predetermined equipment, (phones, PC's, etc.) is positioned for use along with NSE departments Business Continuation Plan.	
4 a.	**ACTIVATE EMERGENCY OPERATIONS CENTER (SECONDARY)** Contact building management and inform them that an emergency situation exists and requires the activation of a conference room for use as an EOC. Have them advise local security to direct all EOC staff to the appropriate location, and ensure that any predetermined equipment, (phones, PC's, etc.) is positioned for use along with NSE departments Business Continuation Plan.	

	NSE PROCEDURES	WHO
5.	**NOTIFY EMERGENCY MANAGEMENT TEAM OF MOBILIZATION** Contact members of the Emergency Management Team (EMT) and instruct them to report to the EOC at the selected location. If possible, use pagers to make initial contact.	
6.	**COORDINATE A DETAILED DAMAGE EVALUATION** Prepare the Damage Assessment Worksheet at the end of this appendix and estimate the extent of the incident/disruption.	
7.	**DECLARE DISASTER** A disaster declaration is a formal decision that empowers the critical business functions and teams to activate their recovery plans. Only NSE departments Executive, or alternate if NSE departments Executive is unavailable, has the authority to declare a disaster. The principle criteria for deciding to declare will be the events impact on the recovery time objectives of NSE department's critical business functions. The exact nature of the disaster will determine which critical business function plans and/or recovery teams will be mobilized. The leader of each mobilized team will be instructed to contact their team membership and mobilize them according to the business continuation plan. In the event that a disaster declaration is unwarranted, the EMT will stand down from the emergency and arrange for the restoration of normal operations.	
8.	**MOBILIZE BUSINESS RECOVERY TEAMS** Based on the nature of the disaster, the EMT will selectively activate the critical business function plans and/or recovery teams.	Team Leaders
9.	**NOTIFY KEY CONTACTS** In addition, the following key individuals should be contacted	

	NSE PROCEDURES		WHO
	Area	**Name**	**Phone Numbers**
	the NSE CIO		
	Human Resources		
	Controllers - Treasury		
	Accounts Payable		
	Corporate Real Estate		
	H = home W = work P = pager C = cellular S = satellite F = fax		
11.	**NOTIFY EMPLOYEES** All employees and staff not previously notified will be contacted by the Emergency Management Team Members per the Notification Tree (see 2.6) and provided with any pertinent instructions to follow.		Team Leaders

Emergency Management Team Notification Tree

Notifier	EMT Role	EMT Member	Numbers	Remarks
	EMT Leader			
	Alternate Leader			
	Alternate Leader			
	Alternate Leader			
	Alternate Leader			
	Alternate Leader			

H = home W = work P = pager C = cellular S = satellite F = fax

Team Action Plans

This section contains specific procedures for the established Business Continuation Teams to follow during the various stages of a disaster.

Each team action plan is intended to provide sufficient information for the respective functions to carry out the required business continuation requirements efficiently.

The success of NSE departments plan will depend largely upon each team's ability to effectively implement the business continuation procedures within their operations.

The primary goal of each team's plan is to identify and address as many issues, concerns, actions, and decisions that will impact post-disaster activities. This will result in a logical systematic approach to dealing with a disruption, which causes business continuation activities to commence. In addition to having a structured process in place, effective implementation of the plan will help reduce confusion, repetition of efforts and communication breakdowns during a disaster response.

The team plan provides member contact information; required resources; contact and vendor information; and procedures for the emergency, recovery, and restoration phases of business continuation. It is the responsibility of each team member to be aware of their individual and team requirements and to update their team's information as required.

The Technology Services area of NSE departments will be used in a support capacity in any emergency. The technical skills of the group will be made available to other areas to ensure that the infrastructure needs of mission critical systems are met.

Emergency Management Team Action Plan

Mission

The Emergency Management Team's (EMT) primary responsibility is to direct and oversee all business continuation activities during implementation of NSE departments plan. Key individuals from all areas (i.e., business functional areas) are the make-up of this team.

Note: Members of the emergency management team representing the business functional areas also serve as team leaders for their respective functional team.

Team Procedures

The emergency management team objectives during the emergency, recovery, and restoration phases of the business continuation plan are as follows:

- To facilitate recovery of NSE department's critical business functions in a timely manner following a declared disaster.
- Evaluate event specific conditions to determine need to declare a disaster and initiate activation of contingency plans.
- Address alternative/exceptions to established contingency plans that may need to be taken.
- Maintain communication with the NSE Corporate Functional Executives throughout emergency, recovery, and restorations phases of contingency operations.
- Coordinate arrangements for travel, where required to support the recovery and restoration of operations.
- Facilitate logistics of setting up supplies, equipment, etc. where needed.

Emergency Phase Procedures

	NSE PROCEDURE	WHO
1.	**ACTIVATE EMERGENCY OPERATIONS CENTER (EOC)** The Emergency Management Team will relocate to the EOC as directed by the team leader (or alternate). Immediate upon arrival at the EOC, the team will need to activate communications. Cell phones, direct lines, etc. should be made operational.	
2.	**REVIEW DAMAGE SURVEY AND DETERMINE NEXT STEPS** Team Leader reviews available information and consults with key team members to determine if declaration will be made. ***ONLY THE TEAM LEADER (OR ALTERNATE) CAN MAKE A DECLARATION.***	
3.	**DECLARE A DISASTER AND ACTIVATE RECOVERY PLANS** Upon declaration, determine which functional areas will be mobilized. If the disaster is limited in nature, only those teams directly affected will be activated. If the disaster has left the building unavailable for an unacceptable period of time, the entire NSE department's business continuation plan will be activated.	
4.	**ARRANGE FOR TRAVEL WHERE NECESSARY**	

	NSE PROCEDURE	WHO
	Assist those employees who will be traveling to remote recovery locations, such as other the NSE locations (e.g., other NSE departments) or non-local vendors.	

Recovery Phase Procedures

	NSE PROCEDURE	WHO
1.	**MONITOR RECOVERY OPERATIONS OF CRITICAL FUNCTIONS** Once the immediate effects of the disaster have been addressed, the Emergency Management Team's primary responsibility will be to monitor individual team plan implementation for: * Ensuring adequate resource distribution to meet business needs. * Coordinating activities with support areas. * Reviewing/approving deviations from established plans.	
2.	**CONTINUE TO PROVIDE STATUS UPDATES** The emergency management team also continue to facilitate the communication process with: • Senior management. • Associates where necessary.	

Restoration Phase Procedures

	NSE PROCEDURE	WHO
1.	**COORDINATE WITH SERVICE PROVIDERS AND THE NSE *departments* STAFF FOR MIGRATION OF WORK TO THE RESTORED (OR NEW) FACILITY**	

	NSE PROCEDURE	WHO
	The Emergency Management Team will oversee the transition of work back to NSE. Working with the functional teams, the EMT should ensure that: • Appropriate equipment is up and operational. • System connections have been reestablished. • Business contacts have been informed. • Appropriate vendors have been notified. • Issues identified during start-up are resolved. • Any temporary operations established during the disaster are ceased.	
2.	**PREPARE FINAL REPORT FOR RECOVERY AND RESTORATION OF NSE departments** Direct the teams to compile a final accounting of the expenses; travel and lodging expenses; replacement costs; overtime; and all other monetary outlays associated with the Business Continuation effort. A final reporting will be made to corporate risk management to ensure all items covered for by the enterprise insurance policies are submitted.	
3.	**REQUEST FINAL STATUS AND RECAP REPORTS** Request that each Team Leader provide the Emergency Management Team with a final Status Report (see example at the end of this appendix) detailing the move, current status and overall business recovery experiences. In addition, request that they develop revisions or other updates to their Team's Action Plan and provide these to NSE departments BCP Planner, so maintenance can be made to the plan document.	

Resource Items

Item	Contact/Location/Phone
Space • Work spaces (staff) including ability for working shifts/overtime.	Work from home

PC Hardware Units • Laptop PCs	With associate
Telecommunications • Phone lines	Associates home lines
Data Communication • Dial-up access requirements.	Pre-loaded on laptops
Critical Systems/Application • *Communications*	Remote access database
Non-System Dependencies • Copy of BCP	Extra copies stored at associate's home and/or car

Mission Critical System - Template (1 per system)

Mission

CRITICAL BUSINESS PROCESSES	RECOVERY TIME OBJECTIVE
Disaster Notification	Immediate
Disaster Response	Immediate

Team Members

	Name	Phone Numbers	Remarks
Team Leader			
Alternate			
Member			
Member			

H = Home; W = Work; C = Cell; P = Pager; S = Satellite

Notification Team Procedures - All Phases

Emergency Phase

	NSE PROCEDURE	WHO
1.	**COORDINATE WITH EMT TO DETERMINE MOST LIKELY OUTAGE PERIOD.** Team leader will be contacted by NSE departments executive and will report to the emergency operation center for information on the estimated duration of the outage and any special concerns that may affect recovery operations.	
2.	**NOTIFY STAFF** Contact staff and advise on status of disruption. If on site, and emergency evacuation is necessary proceed with evacuation and brief staff as soon at it is feasible. If off-site, contact staff according to call tree, to provide nature and status of disruption. All team members should be told if, and where, to meet.	
3.	**SALVAGE ANY WORK IN PROGRESS** Depending on the nature of the disaster, and it is safe and feasible to do so, instruct employees to salvage as many vital records as possible. This will include the saving of electronic documents and an orderly shut down of any electronic equipment. Also any paper or electronic documents that may not be replaceable should be removed from the facility to prevent their destruction.	
4.	**NOTIFY KEY CONTACTS** In coordination with the EMT, notify any key contacts and advise on the situation. Contacts will include:	

	NSE PROCEDURE	WHO
	• Corporate Security - advise of situation. • Vendors - contact applicable vendors as necessary for any alterations to normal business practices.	

Recovery Phase

	NSE PROCEDURE	WHO
1.	**COORDINATE TRANSFER OF WORK** If transfer of work is necessary, contact Corporate Security.	
2.	**COORDINATE WITH OPERATIONS FOR TRANSFER OF WORK** Coordinate with the appropriate contacts (through the EMT) for transfer to the recovery site.	
3.	**IDENTIFY RECOVERY SITE** Determine most appropriate location for recovery site. : • Employee expenses and Incidentals • Lodging and meals • Compensation issues including overtime payment • Temporary reporting structure and responsibilities Employees and management must agree upon the duration of the relocation.	
4.	**FACILITATE STAFF RELOCATION AT RECOVERY SITE** Coordinate with local recovery site staff to configure space and hardware resources for relocated employees at the temporary work site. The following must be addressed: • Work space, including PCs, furniture, phone, fax, copiers, etc. • Hours of operations and possible shift work • Required supplies	

	NSE PROCEDURE	WHO
	• Connectivity with applications and data • Telephone connectivity and voice mail if applicable • Forwarding of mail and parcels for local distribution at the recovery site • Schedule status updates on recovery operations	
5.	**CONTINUE RECOVERY OPERATIONS** Monitor and update distribution of workload to the recovery sites as necessary. Also, determine frequency of status briefings with EMT and conduct as needed.	

Restoration Phase

	NSE PROCEDURE	WHO
1.	**COORDINATE TRANSFER OF WORK BACK TO PERMANENT NSE departments SITE** Based on the status of the restoration, determine when associates and work functions can return to the permanent site. If necessary return may be phased to allow a gradual return to normal. Coordinate with recovery sites for schedule of work transfer. Inform staff members of scheduled move. Notify vendors for mail and other services for resumption of normal operations.	
2.	**RETURN TO NORMAL BUSINESS OPERATIONS** Initiate the migration back to the permanent site. Coordinate replenishment of used supplies and damaged equipment. Any excess supplies and temporary equipment should be returned to its proper place. Verify on-line connectivity is restored.	
3.	**CRITIQUE BUSINESS CONTINUATION PLAN IMPLEMENTATION RESULTS** Assess how well each step of the business continuation plan worked and determine what could have been done better or differently. Modify business continuation plan to correct any deficiencies and reflect strategies that worked. Be sure to	

	NSE PROCEDURE	WHO
	coordinate any changes with the business continuation plan coordinator as per current maintenance policy.	

Resource Items

Item	Contact/Location/Phone
Space • Work spaces (staff) including ability for working shifts/overtime.	Work from home
PC Hardware Units • Laptop PCs	With associate
Telecommunications • Phone lines	Associates home lines
Data Communication • Dial-up access requirements. (RLA access)	Pre-loaded on laptops
Critical Systems/Application	Remote access into E-Mail
Non-System Dependencies • Copy of BCP	Extra copies stored at associates home and/or car

H = Home; W = Work; C = Cell; P = Pager; S = Satellite

Testing and Maintenance

The business continuation plan is a constantly changing document that is never truly "finished". Much of the information it is based on is often obsolete within a short time of its inclusion in the plan.

For this reason, the plan must be reviewed **at least on a quarterly basis** for it to remain a viable document.

All of the major components, from the basic assumptions to the members of the various recovery teams, periodically need to be re-examined to determine whether the information is still correct.

No plan can be relied on unless it is proven effective through testing. The cycle of testing and maintenance is never ending. This chapter details the overall strategy for maintaining the Business Continuation Plan, including testing, maintenance, and distribution.

Maintenance Schedule

Most maintenance to the plan will be routine in nature. Changes in employees will require updates on contact information and staff lists. A review of this information is simple and should be scheduled often. Other changes, such as in risk exposure, critical function processing, or recovery strategy will usually occur less often and involve more time for review and analysis. While the frequency and subject of the scheduled reviews should be developed around the specific needs of the Business Continuation Plan in question, the following outline will serve as an effective starting point:

- ***Quarterly Reviews***: All employee listings, including functional area team membership, should be reviewed to ensure that staff names and contact information is correct.

- ***Semi-Annual Reviews***: This type of review examines the basis for the Business Continuation Plan. The business impact analysis, risk assessment, and selected strategies should all be evaluated to ensure their applicability with the existing plan.

- ***Annual Reviews***: Once a year, the entire Business Continuation Plan should be reviewed to determine if any changes have been made and, if so, document these changes. This is usually done in conjunction with a test or exercise of the plan so that any proposed changes can be validated. An added benefit of the test is that participants are trained in responding to a disaster or other disruption.

Event and Situation Triggered Reviews and Actions

There may be certain business-related events that may occur which may affect the NSE departments Business Continuation Plan. For example, a change in application dependency from mainframe to client server would necessitate reviewing the recovery strategies, testing strategies

and possibly the list of contacts and vendors. Another example of this is if a consolidation of work processes occurred which would require a review of the selected recovery strategies, resource requirements and the functional area recovery team members.

The following table includes many events that may necessitate a Maintenance Review. While this list is extensive, there may be additional conditions not listed that could also justify a review:

EVENT/SITUATION	ACTIONS TAKEN
Is there a change to a current critical function?	Review all information associated with the function (RTO, processes, procedures, etc.) and revise as needed
Does the new or revised function affect the recovery strategy?	If so, it should be revised
Is this a new critical function?	Review all information associated with the function (RTO, processes, procedures, etc.) and add to plan
Does the new critical function impact any other critical functions?	If so, then determine it's impact and make any adjustments as needed
Does the new or revised function have any new system dependencies?	If so, these should be included in the dependency provider's plan or section
Is the new or revised function performed in a new location?	If so, it should be revised
Are there any new critical personnel?	If so, revise any pertinent contact information
Has there been a change to an existing strategy?	If so, modify the strategy description in Chapter 1
Has there been a change to any of the following... a. **Critical Function** b. **Processes and Procedures** c. **Workspace Requirements** d. **Communication Equipment Needs** e. **Hardware Needs** f. **Software Needs**	If so, make the necessary revisions

EVENT/SITUATION	ACTIONS TAKEN
g. **Office Equipment Needs** h. **Special Supplies** i. **Forms and Documents** j. **Manuals** k. **Vital Documents Inventory** l. **Employee Information** m. **Critical Personnel** n. **Mail Services** o. **Regulatory Agency Information** p. **Emergency Contacts**	
Has a new or changed risk been identified for your critical business functions or location?	If so, re-evaluate the potential business impact and determine if the existing strategies are sufficient
Is there a new vendor for a necessary service or product?	If so, make the necessary revisions
Is this a change in priority to an existing vendor?	If so, make the necessary revisions
Is there new hardware/software associated with the vendor?	If so, determine if present procedures are applicable and if modifications are needed
Is there a new assumption or a change to an existing assumption? (An example of a change in assumption would be the existing assumption that "qualified personnel in sufficient quantities would be available" may no longer be true)	If so, then revise Chapter 1 of the plan to reflect the change
Does the change in assumption affect the Business Impact Analysis?	If so, the Business Impact Analysis should be revisited and revised
Does the new or revised assumption involve new or different personnel?	If so, make the necessary revisions
Does the new or revised assumption affect the recovery strategy?	If so, then the strategy needs to be revised
How does the new or revised assumption affect	Review the Resource requirements and

EVENT/SITUATION	ACTIONS TAKEN
the currently listed Resource requirements?	make any needed adjustments
Has there been a change to the Plan Maintenance	If so, then revise Chapter 4 of the plan to reflect the change
Are there any new associates in need of training on the Business Continuation Plan?	If so, the Plan Coordinator should insure that the new member receives training from his or her respective team leader or manager
Does the new member need a current copy of the Business Continuation Plan?	If so, then the Plan Coordinator should ensure that the new member receives it

It should not be the Business Continuation Planner's sole responsibility to uncover changes during his/her scheduled review. If a change in the organization occurs that is known to have an impact on the Business Continuation Plan, the appropriate associate should bring it to the Planner's attention that will review and document the change.

Testing

The only way to ensure the viability of a plan is through initial and periodic testing. Initial testing is necessary to verify the accuracy of all documented information. It is also necessary in order to demonstrate the plan's completeness and ensure that no steps or procedures have been overlooked. After this first test, periodic tests should be scheduled to accommodate any changes in personnel or the organization. Any improvements identified through testing should be incorporated into the plan to be re-tested in the future.

The three main objectives of any test are to:

- Ensure that the Business Continuation Plan is functional;
- Train staff to become familiar with their responsibilities during a disaster; and,
- Identify areas for improvement.

The type of test selected will depend on the specific objectives chosen, as well as the level of preparedness possessed by employees and management. In general, there are four varieties of business continuation plan testing. These are:

- Static or verification;
- "Table-top" validation;
- Walk through Simulation; and,
- Dynamic Simulation.

STATIC (VERIFICATION) TESTS

Individuals also know static tests as verification tests since they only involve checking and updating written plan components. Static tests will be conducted for the following:

- Verify employee contact information
- Verify vendor/resource contact information

"TABLE-TOP" OR VALIDATION TESTS

"Table-Top" or validation tests are used to confirm the procedures used by individuals or teams. These tests typically involve group discussions on the effectiveness of the procedures as they apply to the team objectives. Disaster responses are limited to only those procedures documented in the current Business Continuation Plan. This allows the participants to verify the fidelity of the present plan without relying on undocumented actions. Validation tests will be conducted for the following:

- As the initial plan testing method for new business continuation plans
- Upon addition or revision of existing team objectives
- When substantial changes to normal operating procedures has occurred

WALK THROUGH SIMULATION TESTS

A walk through simulation test is a representation of disaster conditions. Participants are presented with a disaster scenario and are asked to describe in detail their combined response to this event. In many ways it is similar to the Validation Test, but here the participants actually perform selected tasks and physically occupy the designated EOC and recovery locations.

DYNAMIC SIMULATION TESTS

Dynamic tests are operational in nature and actually involve bringing up critical applications and production processes in alternate locations. Dynamic tests are required only when recovery procedures cannot be suitably developed with only the other three test types. These tests may or may not be announced. To promote confidence in the ability of the company to recover from any emergency situation, the scenarios should be varied, and contain as much realism as possible. Observers should be designated to take notes on the groups performance, since test participants should be dedicated to their actual tasks. The observer will identify problems that occur as a result of missing, incomplete or inaccurate plan information. Once the scenario is completed, the group will review the deficiencies and propose the appropriate revisions.

This form of testing is useful in determining the reactive capability of a team to differing scenarios.

Examples of Dynamic Simulation Tests include:

- Fire and evacuation drills
- MIS environment re-creation within the existing facility or alternate location in parallel to existing data processing
- Plans that involve the use of outside vendors

As these exercises themselves can lead to major disruption in normal operations, they should only be conducted with adequate prior planning and notice and the full cooperation of Senior Management.

All participants should be notified if a test is being conducted. Only Dynamic Simulation tests may be unannounced and then only after sufficient previous tests have been successful and senior management approves it.

All tests, regardless of whether they are announced or not, should be adequately prepared in advance. A comprehensive test program should be developed, with time frames established for each step of the process. **One individual should be responsible for coordinating the testing program.**

A comprehensive test program should include:

- General procedures for the execution of the test
- Contingency procedures should there be a problem
- Termination points of the test, regardless if a task has been completed

- Operation shut-down procedures
- Operation recovery procedures
- Retrieval of vital records, information, supplies, etc.

Business Continuation Plan Updates and Distribution

It is the responsibility of the Business Continuation Planner to ensure that once changes have been identified, the plan is appropriately revised, discussed with the relevant personnel and distributed on a timely basis.

The distribution of the plan document itself must comply with the distribution policy as outlined in Chapter 1. As the document is confidential, it must be safeguarded to protect the personal and proprietary information it contains. Distribution must be controlled and accountable.

Distribution of the plan in its entirety is generally limited to the site Business Continuation Planner, senior NSE department's management, members of the Enterprise Business Continuation Office, and authorized internal and external audit/compliance parties. Various sections of the plan may be distributed to individuals who are involved in particular aspects of business continuation but may not have a need to view the complete document. Team leaders are responsible for the distribution of functional area plans to their respective team members.

Plan copies are distributed after any revision is published, with any obsolete copies returned to the Business Continuation Planner for destruction. In order to facilitate this process, the Planner maintains a Distribution Log to track outstanding copies and list recipients.

Plan recipients are informed on the confidential nature of the document and are required to sign the Distribution Log to verify their knowledge of this.

Support Contents

Facilities Emergency Procedures
Master Employee Listing
Damage Assessment Checklist
Directions to Emergency Operations Centers
Approved Press Release
Recovery Status Report
Testing and Maintenance Schedules

Test Results
Test Guides
Maintenance Log
Maintenance Request
Reciprocal Agreements
Document Control Sheet
Dependency Roll-Up
Vital Record Summary
Corporate Risk Management Policy

!

Forms, Checklists & Reports

!

"#$ #%&#''&''$ &() *+&*,-.')

Structure

Nature of Disruption:_____

Type of Damage: _____

_____

_____

Rate Severity: ☐ None ☐ Slight ☐ Bad ☐ Total Loss

Rate Duration: ☐ 12 hrs ☐ 24 hrs ☐ 2 Days ☐ 1 Week ☐ 2 Weeks ☐ Longer

Input received from:_____

Electrical

Nature of Disruption:_____

Type of Damage: _____

_____

_____

Rate Severity: ☐ None ☐ Slight ☐ Bad ☐ Total Loss

Rate Duration: ☐ 12 hrs ☐ 24 hrs ☐ 2 Days ☐ 1 Week ☐ 2 Weeks ☐ Longer

Input received from:_____

Communications

Nature of Disruption:_____

Type of Damage: _____

_____

_____

Rate Severity: ☐ None ☐ Slight ☐ Bad ☐ Total Loss

Rate Duration: ☐ 12 hrs ☐ 24 hrs ☐ 2 Days ☐ 1 Week ☐ 2 Weeks ☐ Longer

Input received from:_____

Data Center

Nature of Disruption:_____

Type of Damage: _____

_____

_____

Rate Severity: ☐ None ☐ Slight ☐ Bad ☐ Total Loss

Rate Duration: ☐ 12 hrs ☐ 24 hrs ☐ 2 Days ☐ 1 Week ☐ 2 Weeks ☐ Longer

Input received from:_____

Heating/Ventilating/Air Conditioning

Nature of Disruption:_____

Type of Damage: _____

_____

_____

Rate Severity: ☐ None ☐ Slight ☐ Bad ☐ Total Loss

Rate Duration: ☐ 12 hrs ☐ 24 hrs ☐ 2 Days ☐ 1 Week ☐ 2 Weeks ☐ Longer

Input received from:_____

Environmental

Nature of Disruption:_____

Type of Damage: _____

_____

_____

Rate Severity: ☐ None ☐ Slight ☐ Bad ☐ Total Loss

Rate Duration: ☐ 12 hrs ☐ 24 hrs ☐ 2 Days ☐ 1 Week ☐ 2 Weeks ☐ Longer

Input received from:_____

General Offices

Nature of Disruption:_____

Type of Damage: _____

_____

_____

Rate Severity: ☐ None ☐ Slight ☐ Bad ☐ Total Loss

Rate Duration: ☐ 12 hrs ☐ 24 hrs ☐ 2 Days ☐ 1 Week ☐ 2 Weeks ☐ Longer

Input received from:_____

RECOVERY STATUS REPORT

The Recovery Status Report is completed by each recovery team member to document his or her activities. This checkpoint report should be given to the Team Leader. All of the requested information is to be completed for each to enable monitoring the progress of the recovery. The Emergency Management Team uses this information to provide briefings to senior management and to analyze the recovery once normal operations are restored.

Name:_____ Team Name:_____

Title:_____ Date/Time:_____

Subject/Location: _____

Findings/Observations: _____

_____

_____

_____

_____

Recommendations: _____

_____

_____

APPENDIX 11

MAINTENANCE LOG

The chart below will be used to record when maintenance is performed on the various sections and Team Action Plans that make up this Business continuation Plan document. Team Leaders or other responsible individuals will initial and indicate the date of each update on the lines that correspond to their respective section or team.

Date		New Version		Description of Activity		Next Review

PRESS RELEASE

Press Releases / Media Statements to be used at time of disaster or serious disruption:

"A (fire, power outage, etc.) has temporarily disrupted operations at the NSE located in _____. (No, some, exact count) employees in the facility at the time of the event were injured (and were taken to _____ for treatment.)

While this facility sustained (moderate or severe) damage, our emergency and business continuation plans have been activated and are progressing according to schedule. We are striving to minimize any disruption of services for our customers, and will return to normal operations as soon as possible.

As additional information and updates concerning our resumed operations become available you may contact our spokesperson, (spokesperson)at (_) ___-_____."

A list should be available in all departments with the names of all staff who are trained in CPR and First Aid.

Emergency Services Numbers:

It is necessary to maintain a list, with telephone numbers for emergency services. The list could look as follows:

PHONE	TYPE OF SERVICE	CONTACT PERSON(S)	NUMBER
Police Dept.			
Fire Dept.			
Ambulance			
Health Dept.			
Poison Control			
Security Dept.			
Sheriff			

It is also useful to maintain a list of experts:

TITLE/ NAME	PHONE ADDRESS	NUMBER
Architect		
Carpenter		
Chemist		
Computer Engineer		
Electrician		
Fumigation		

Insurance Agent _____

Janitorial Service _____

Legal Advisor _____

Locksmith _____

Pest Control _____

Plumber _____

Telephone Co. _____

Utilities:

Gas _____

Electric _____

Deep Freeze Facility _____

Vacuum or Freeze drying facility _____

Note: A list should be maintained of organizations and services which could be called upon as necessary. A sampling of these could be:

Emergency Procedures & Instructions

Emergency Instruction in Case of EARTHQUAKE

Follow instructions given by [name of local agency] or:

a. During the shaking:
   - Remain where you are.
   - If you are indoors, take cover under a desk, heavy table, or stand in a doorway, hallway or by a wall.
   - Move away from glass and falling objects.

- If you are outdoors, move away from power poles or lines, lamp posts and tall buildings.

b. After the shaking: Abide by local guidelines, or follow instructionsgiven by local authorities.

c. When you have, or are given, access to the facility:

- Check for fire or fire damage.
- Check for flooding or water damage.

Emergency Instructions in Case of FIRE:

a. Activate the ALARM, unless the fire is small and can easily be controlled. Evacuate the area.

b. Call the Fire Department.

c. Fight the fire **ONLY IF:**

- You know how.
- The fire is small.
- Confined to the area where it started.
- You have a way out.
- You can work with your back to the exit.
- You have the right type of extinguisher.
- You feel confident that you can operate it effectively.

d. **DO NOT** fight the fire if:

- You have any doubts about fighting it.
- It is spreading beyond the area where it started.
- It could block your escape route.

e. After you have taken the above steps:Notify the administration:

Title/Name _____ work_____ home_____ or

Assistant Name _____ work_____ home_____ or

Disaster Recovery Coordinator:

Name _____ work_____ home_____

f. If they cannot be reached, call the persons listed below, in the order listed, until you reach someone:

Recovery Specialist Name _____
work_____ home_____

Disaster Recovery Team Member_____ home_____

Head of afflicted area Name _____ home_____

g. After the fire:
- Look for water damaged materials.
- Look for smoke, soot, dirt on materials.
- Look for fallen materials.

Plan Recovery:

a. **Call for assistance** giving dress code and meeting point:
- Disaster Recovery personnel, and other library staff as needed for in-house salvage of materials.
- Service-providers for pack-out.
- Neighboring libraries or volunteers to assist in a major disaster.

b. **Get supplies** or assign someone to:
- Retrieve from in-house containers.
- Request from institutional or network storage facilities. [Contact person or Appendix __]
- Order from commercial vendors.

Appendix ___: Supplies/Suppliers: in-house, off-site, vendors.

Appendix ___: Open purchase order which can be duplicated in emergencies.

c. Prepare staging area as near as possible to disaster area and with best access to supplies and shipping (if required).
- Have table or other work surfaces.
- Have supplies (boxes and freezer paper, set up on a paper spool to tear off) delivered close to the area.
- Observe safety precautions for workers, take security measures for materials, or, request assistance from (name and phone # of health and safety officer) and from (name and phone # of security agency) if circumstances, extent of project or value of materials, warrant it.

d. **Assign Responsibilities**:
- Name group leaders.
- Assign helpers to groups according to skill or experience.

- Divide the work among groups: searchers/ transporters of wet materials, and wrappers/ boxers. Transfer workers from one task to another as necessary to avoid exhaustion and stress.

e. **Supervise the operation**:

- Act as liaison and public relations officer.
- Revise priorities/procedures as deemed necessary.
- Contact the (names and phone #'s of preferred document reprocessor, consultant, mover, freezer facility) needed and arrange for appropriate contracts.

Restoration Actions & Procedure

Disaster Recovery Considerations

Freezing, vacuum drying, and vacuum freeze drying

(1) Background: Research and case studies have shown that large quantities of water damaged library and archival materials can be stabilized and salvaged when frozen and stored at low temperatures (ideally -20 F). Freezing allows the institution time to plan, organize, control and coordinate their disaster recovery and drying plans. Freezing is not a drying method and will not kill mold spores. It does give the library time to plan and organize, and minimizes the damage to the materials. Vacuum drying and vacuum freeze drying are other alternatives for freezing and drying large quantities of damaged materials.

(2) Definitions:

- Freezing: this method uses a self-defrosting fast freezer that has the capacity to freeze items very quickly, at temperatures below -10 F. This method is suitable for non-coated stock and smaller quantities. Items must be left in the freezer from several weeks to several months. As staff time and space permit, items can be taken out of the freezer and air dried before they are returned to their regular shelves.

- Vacuum drying: this method uses a vacuum thermal-drying chamber. Wet or frozen items are placed in the chamber, a vacuum is drawn, heat is introduced, and the materials are dried. The temperature stays above 32 F. This method is good for large numbers of materials, is easier and more cost effective than air drying, and is good for extensively water damaged items. Unfortunately this method often produces extreme distortion of books requiring them to be rebound. This process tends to also cause coated papers to stick together.

- Vacuum freeze drying: in this method frozen books and records are placed in a vacuum chamber. A vacuum is drawn and carefully controlled heat is applied. The temperature is kept below 32 F. This

combination causes the frozen water to go directly from that state to the gaseous state. This process of sublimation eliminates further damage to the materials through distortion, bleeding and sticking together. It is an effective way to handle and dry large quantities of materials. The main drawback is the cost.

Dehumidification:

(1) Definition - to remove the moisture from the air, the collection, and the building using large commercial dehumidifiers.

(2) Benefits and Disadvantages - This method is fairly new in the library and archival field, though it has been used extensively in office buildings. A major benefit is that staff does not need to remove and box any items, all of the work is done in-house. If it is not done within 24 hours though, mold & mildew can set in, and swelling and adhesion has started. Also additional testing and reports on this method still need to be conducted and checked into before an institution decides on this option.

2. Smoke, Soot, and Char Damage: Smoke damage is usually irreversible, but it is possible to remove some of the surface soot and char by using some of the following methods. The paper should be completely dry and in good condition. Consult a conservator for rare and valuable items.

- Remove soot from paper by use of chemical sponges, erasers, or a dry cleaner such as Groomstik or Absorene Paper & Book Cleaner which is available from archival supply companies such as Light Impressions, Archival Quality Materials, or Demco.
    - Use chemical sponges in a gentle, brushing motion. Do not scrub since this will damage the paper. Try a test page.
    - Erasers or a dry cleaner also need to be used with a gentle brushing motion. Use an artist brush to remove the rubbings. One source reported that pink pearl erasers worked best. Another suggestion is to use extra fine steel wool to clean soot from leather bindings. (Abbey Newsletter, October, 1986).
- Char can be trimmed by using paper shears, razor blades, or scissors.

Consider the aesthetics of a damaged item prior to returning it to the shelf. Some suggestions for improving appearances are: rebinding, phase boxes, file folders, or adding a cover or jacket.

Biopredation:

Mold and Mildew: Mold and mildew are fungi that form under certain conditions. If untreated they can severely damage library material. Conditions are particularly favorable when the disaster involves water, but they can form at any time.

(1) Factors favorable for the development of mold and mildew.

- Temperature (+75 F).
- Moisture (+60% humidity).
- Dark.
- Little air circulation.

(2) Steps to take:

- Transfer all infested material to an isolation room.
- If number is large, prepare for freezing.
- Thoroughly clean and sterilize infected area.

(3) Mass methods (DO NOT ATTEMPT WITHOUT EXPERT ADVICE. MAY BE HAZARDOUS TO HEALTH OF WORKERS):

- Fungicidal fogging with Thymol
- Fumigation with Ethylene Oxide

(4) Treatment of individual items infested with mold and mildew:

- Treatment of papers and binders
    - Supplies needed:
      Blotters
      Cheesecloth
      Lysol spray
      Q-tips
      Gloves (optional)
      Mask (optional)
      Wax paper (optional)
- Lay the item on a clean white blotter. Wet the Q-tip with the Lysol and test ink to see if it is damaged by Lysol. If it is, stop!
- Lightly spray item with Lysol. Use wax paper to cover uninfected areas.

- Use cheesecloth to carefully wipe or blot the infected area. Repeat if necessary. DO NOT SCRUB!
- Let item dry while working on the next one.
- Surface cleaning for flat papers or books.
    - Supplies:
      Dry cleaning pads or powder
      Weight(s)
      Soft, wide brush
      Scrap paper
      Wastebasket
      Air bulb (optional)
      Mask (optional)
      Gloves (optional)

- Examine item to see if it is completely dry. Do not proceed if paper is not in good condition, or is flaking, so that the item will not be scratched or damaged. If indoubt get expert advice.
- Lay item on clean working surface. Use gloves or make certain hands are clean.
- Lay item down and use weight to hold it in place. Use air bulb to blow away large pieces.
- Pretest on a small area before continuing.
- Sprinkle dry cleaning powder on item to be cleaned. Gently roll powder with your fingertip over stained areas. Powder picks up surface dirt and turns black or grey.
- Brush away powder from the center out to the edges. Do not leave any powder residue on item.

Insects and rodents:

- Identify pest.
- Consult with a professional. Remember that anything used to exterminate should be considered hazardous. Don't proceed unless you have thoroughly discussed the situation with several professionals, including safety experts.
- Try to locate the way pests entered and carefully block their entrance way.

Dirt

Before cleaning a book or paper, make sure that it is completely dry and is not fragile or brittle. Surface dirt can be removed by gently brushing away with a soft artist brush, by use of a special eraser, or by use of a dry cleaner such as Groomstick or Absorene Paper & Book Cleaner.

Mud on books can be washed off if the books are already thoroughly wet and won't be damaged further by contact with water. Otherwise, mud on fairly dry books can be dried and then cleaned off. For thoroughly wet books, use a tank with clear, running water. Immerse the book in the water. Keep the book closed and clean with a gentle, dabbing motion of a soft sponge. Avoid brushing and rubbing. Hard to remove stains can be dealt with by a professional conservator after the book dries.

Recovery & Completion Procedures

Housekeeping and Rehabilitation:

a. Building: The building should have passed an official safety inspection. The following items should be thoroughly checked:

- All areas of the building cleaned and sterilized. Make sure it has thoroughly dried.
- Heating and air conditioning systems should be in full working order.
- Fire detection and extinguishing systems should be in fullworking order.
- Security systems should be in full working order.
- Repairs to structure and equipment should be complete and building certified for occupation.

b. **Collection:**

- Select area for rehabilitation for all material damaged by water.
- Do daily random checks for mold.
- Assess material for replacement or for further treatment.
- After six months, material may be returned to collection.
- Only thoroughly dry material should be returned.
- Material should be thoroughly examined by an expert.
- Check that markings are correct.
- Maintain accurate records.

Assessment and Revision:

a. Purpose:

Every disaster plan needs to be established according to the needs and demands of the institution that it is meant to serve. In addition, it is very important that the disaster plan cover all types of disasters, big and small with clear instruction on what needs to be done. The plan must be reviewed frequently so that any necessary changes and updates can be made.

b. Disaster Assessment:

Management staff, should have a simple easy to follow checklist that can help them to make a final assessment of how well they met the disaster and were able to deal with it. Some checklist items could be:

- Staff performance.
- Adequate supplies.
- Cooperation between departments, division, outside help.
- Adequate record keeping.
- How efficiently were things handled? How can they be improved?
- (Listing of unexpected problems and their solutions.

c. Revision: Using disaster drills, brainstorming sessions, and disaster follow-up assessments, staff should periodically review and update disaster plans so that they will be adequate to meet the needs of the institution when they are needed.

APPENDIX 12

12. Sample - NSE Disaster Recovery Procedure Guide

This Appendix provides a sample DR guide for NSE that includes:

- Emergency Levels
- Emergency Response Team Actions & Instructions;
- Hazards and Threats with profiles for each and
- First Response Steps to Take;
- Configuration setup for the Alternate Site; Recovery Priorities; and,
- Checklist of Actions to take

Note:This guide is provided to enhance NSE DR planning. It is not intended to be a complete work. Not every recovery function is represented and not every plan component is presented. Areas of this Appendix have been highlighted (see Table of Contents) for management awareness.

1.0 Overview

1.1 Policy Statement

It is the Policy of NSE (**"NSE"**) to maintain a comprehensive Business Continuity Plan for all critical organization functions. Each department head is responsible for ensuring compliance with this policy and that their respective plan component is tested no less than annually. **The** NSE Disaster Recovery efforts exercise reasonable measures to protect employees, safeguard assets, and client accounts.

1.2 Introduction

This plan was specifically designed to guide **NSE** through a recovery effort of specifically identified organization functions. At the onset of an emergency condition, **NSE** employees and resources will respond quickly to any condition, which could affect **NSE**'s ability to perform its critical organization functions.

The procedures contained within have been designed to provide clear, concise and essential directions to recover from varying degrees of organization interruptions and disasters.

1.3 Confidentiality Statement

This document is classified as the confidential property of **NSE**. Due to the sensitive nature of the information contained herein, this document is available only to those persons who have been

designated as plan participants, assigned membership to one of the **NSE** recovery teams, or who otherwise play a direct role in the recovery process.
This document remains the property of **NSE** and may be repossessed at any time. Unauthorized use or duplication of this document is strictly prohibited and may result in disciplinary action and/or civil prosecution.

1.4 Document Distribution

Each plan recipient will receive and maintain two (2) copies of the disaster recovery document; one copy will be kept in the plan recipient's work area; the second copy will be kept at the plan recipient's residence. Each document has a control number to track its distribution. Replacement documents and additional copies may be obtained from **NSE**'s Disaster Recovery Manager.

1.5 Document Reclamation

Plan recipients who cease to be an active member of a disaster recovery team or an employee of **NSE** must surrender both copies of their disaster recovery document to the Disaster Recovery Manager. **NSE** reserves any and all rights to pursue the return of these documents.

1.6 Plan Revision Date

The latest document revision date appears in the lower right hand corner of the footer. This date indicates the most published date of the plan section.

1.7 Defined Scenario

A disaster is defined as a disruption of normal organization functions where the expected time for returning to normalcy would seriously impact **NSE**'s ability to maintain customer commitments and regulatory compliance. **NSE's** recovery and restoration program is designed to support a recovery effort where **NSE** would not have access to its facilities and data at the onset of the emergency condition.

1.8 Recovery Objectives

The **NSE** Plan was written with the following objectives:

- To ensure the life/safety of all **NSE** employees throughout the emergency condition, disaster declaration, and recovery process.
- To reestablish the essential organization related services provided by **NSE** within their required recovery window as identified in the recovery portfolio in Section 2 at the declaration of disaster.

- To suspend all non-essential activities until normal and full organization functions have been restored.

- To mitigate the impact to **NSE's** customers through the rapid implementation of effective recovery strategies as defined herein.

- To reduce confusion and misinformation by providing a clearly defined command and control structure.

- To consider relocation of personnel and facilities as a recovery strategy of last resort.

1.9 Plan Exclusions

The **NSE Business Continuity Plan** was developed with the following exclusions:

- Succession of Management
- Restoration of the Primary Facilities

1.10 Plan Assumptions

NSE's Business Continuity Plan was developed under certain assumptions in order for the plan to address a broad spectrum of disaster scenarios. These assumptions are:

- **NSE**'s recovery efforts are based on the premise that any resources required for the restoration of critical organization functions will reside outside of the primary facility.

- Any vital records required for recovery can be either retrieved or recreated from an off-site location and moved to the recovery facility within 24 hours.

1.11 Declaration Initiatives

NSE's decision process for implementing any of the three levels of recovery strategies to support the restoration of critical organization functions are based on the following declaration initiatives:

- Every reasonable effort has been made to provide critical services to **NSE**'s customers by first attempting to restore the primary facility and / or operate using intra-day procedures.

- After all reasonable efforts have failed to restore the primary facility, and using document procedures severely degrades client support, **NSE** would invoke a recovery strategy that requires the relocation of personnel and resources to an alternate recovery facility.

- If the outage will clearly extended past the acceptable period of time identified in the Recovery Portfolio, (see Section 2) a declaration of disaster will immediately be made.

1.12 Recovery Strategies

In order to facilitate a recovery regardless of the type or duration of disaster, **NSE** has implemented multiple recovery strategies.

Emergency Levels

These strategies are categorized into three (3) emergency levels. Each level is designed to provide an effective recovery solution equally matched to the duration of the emergency condition.

- **LEVEL 1: SHORT-TERM OUTAGE (FAIL-OVER) - INTRA-DAY**

  A short-term outage is defined as the period of time **NSE** does not require computerized operations, or where an outage window of the same day or less would not allow adequate time to restore / utilize automated recovery operations.

- **LEVEL 2: MEDIUM-TERM OUTAGE (TEMPORARY) - UP TO SIX WEEKS**

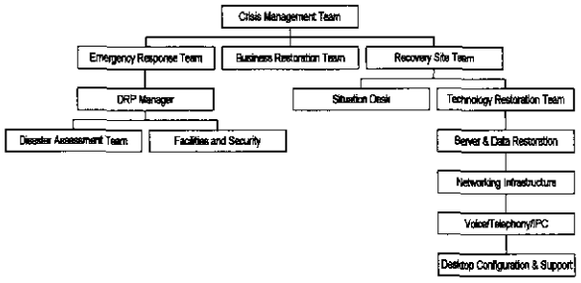
  A medium-term outage is defined as the period of time that **NSE** will execute its formal disaster recovery strategy, which includes actually declaring a disaster. A disaster may either be declared company wide or only for the effected department or building. The decision to declare a disaster will be based on the amount of time / expense that is required to implement the formal recovery and the anticipated impact to **NSE**'s organization over this period.

- **LEVEL 3: LONG-TERM OUTAGE (RELOCATION) - 6 WEEKS OR MORE**

A long-term outage is defined, as the period of time that **NSE** will exceed the allowed occupancy time of its primary recovery strategy. During this phase of recovery, **NSE** will initiate a physical move of personnel and resources.

1.13 Team Overview

During an emergency, each team member contributes the skills used in everyday work to the overall response.



1.14 Team Charters

Crisis Management Team - The CMT is comprised of senior **NSE** management and is responsible for authorizing declarations of disaster, emergency investment strategy, approving public release of information, and ensuring donors and constituents are informed.

Emergency Response Team - The ERT is first on scene to assess the damage caused by the disaster or ensure precautionary measures are taken in light of <u>any</u> impending disaster (e.g. inclement weather, etc.) Once the ERT determines the extent of the disaster, they will either order an evacuation of the facility or work with facilities to mitigate the effects to **NSE**.

Recovery Site Team - The RST Team provides enterprise-level support for both the physical site and technology issues. The members of this team will ensure that the alternate site is ready,

and adequate for arriving recovery personnel. The RST will be the first at a meeting point or alternate site in order to register arriving personnel.

Business Restoration Team – The BRT'S consist of personnel from each **NSE** area deemed critical to the continuation of **NSE**. The captains of the BRT get updated status from the ERT and the RST to pass on to their team members to ensure prompt recovery of each department.

2.0 Recovery Strategies

Emergency Response Team Actions & Instructions

The following are the identified recovery strategies for the organization:

RECOVERY AREA:	PRIMARY STRATEGY:	BACKUP STRATEGY:
Office Space	Mobilization Time: ( )	**Mobilization Time: ( )**
Phone System	Mobilization Time: ( )	**Mobilization Time: ( )**
Network Recovery	Mobilization Time: ( )	**Mobilization Time: ( )**
Server Recovery	Mobilization Time: ( )	**Mobilization Time: ( )**

RECOVERY AREA:	PRIMARY STRATEGY:	BACKUP STRATEGY:
Desktop Recovery	**Mobilization Time: ( )**	**Mobilization Time: ( )**
Office Furniture	**Mobilization Time: ( )**	**Mobilization Time: ( )**
Office Equipment	Mobilization Time: ( )	**Mobilization Time: ( )**
Applications	Mobilization Time: ( )	**Mobilization Time: ( )**
Databases	Mobilization Time: ( )	**Mobilization Time: ( )**
Service Providers	Mobilization Time: ( )	**Mobilization Time: ( )**
Employees	**Mobilization Time: ( )**	**Mobilization Time: ( )**

RECOVERY AREA:	PRIMARY STRATEGY:	BACKUP STRATEGY:

2.1 Emergency Phone Numbers

Complete the following to ensure that you have identified all the

Emergency services

1. Police: (___) ___ - _____
2. Fire: (___) ___ - _____
3. Alarm Company: (___) ___ - _____
4. Ambulance: (___) ___ - _____

Communications

1. Local Telco: (___) ___ - _____
2. Long distance carrier: (___) ___ - _____
3. Direct dial numbers: (___) ___ - _____

   (___) ___ - _____

Weather information

1. NOAA: (___) ___ - _____
2. Radio station:
3. Weather channel:
4. Weather channel: https//:www.weather.com

Maintenance & repair

1. Janitorial: (___) ___ - _____
2. HVAC: (___) ___ - _____
3. Electrical: (___) ___ - _____
4. Glazer: (___) ___ - _____
5. Carpentry: (___) ___ - _____
6. Plumbing: (___) ___ - _____

Logistics

1. Travel agent: (___) ___ - _____
2. Express shipping: (___) ___ - _____
3. Taxi/limo service: (___) ___ - _____
4. Charter air service: (___) ___ - _____

IT services

1. Hardware VAR: (___) ___ - _____
2. Software VAR: (___) ___ - _____
3. Network equipment: (___) ___ - _____
4. Server quick-ship: (___) ___ - _____
5. Desktop quick-ship: (___) ___ - _____

Utilities

1. Electrical: (___) ___ - _____
2. Gas: (___) ___ - _____

3. Water: (___) ___ - _____
4. Sewer: (___) ___ - _____
5. Sanitation: (___) ___ - _____

Employee assistance

1. Child care: (___) ___ - _____
2. Elderly care: (___) ___ - _____
3. Concierge services: (___) ___ - _____
4. Pet care: (___) ___ - _____

2.3 Threat Profile

Hazards and Threat Profiles and Actions

HAZARD:	PROFILE OF HAZARD:	FIRST RESPONSE:
Floods	In several areas of Nigeria, unusually heavy rains may cause "flash" floods. Small creeks, gullies, dry streambeds, ravines, culverts or even low lying round frequently flood quickly. In such situations, people are endangered before any warning can be given.	Step 1: Monitor flood advisories Step 2: Determine flood potential Step 3: Determine employees at risk Step 4: Pre-stage emergency power generating equipment Step 5: Assess damage
Tornadoes	Tornadoes are violent rotating columns of air, which descend from severe thunderstorm cloud systems. They are normally short-lived local storms containing high-speed winds usually rotating in a counter-clockwise direction. These are often observable as a funnel-shaped appendage to a thunderstorm cloud. The funnel is initially composed to nothing more than condensed water vapor.	Step 1: Monitor weather conditions Step 2: Notify employees of potential of severe weather Step 3: Power off equipment Step 4: Shut off utilities (power and gas) Step 5: Instruct employees to assume protective posture Step 6: Assess damage once storm passes Step 7: Assist affected employees

HAZARD:	PROFILE OF HAZARD:	FIRST RESPONSE:
	It usually picks up dust and debris, which eventually darkens the entire funnel. A tornado can cause damage even though the funnel does not appear to touch the ground.	
Hurricanes/ Monsoons	Nigeria is a coastal area and monsoons do affect our area.	Step 1: Power-off all equipment Step 2: Listen to advisories Step 3: Evacuate area, if flooding is possible Step 4: Check gas, water and electrical lines for damage Step 5: Do not use telephones, in the event of severe lightning Step 6: Assess damage
Earthquakes	An earthquake is the shaking, or trembling, of the earth's crust, caused by underground volcanic forces of breaking and shifting rock beneath the earth's surface.	Step 1: Shut off utilities Step 2: Evacuate building if necessary Step 3: Account for all personnel Step 4: Determine impact of organization disruption
Power Failures	Power failures occur in many parts of the country throughout the year. They can be caused by storms, lightning or construction equipment digging in the wrong location. For whatever the reason, power outages in a major metropolitan area can severely impact the entire community.	Step 1: Wait 5-10 minutes Step 2: Power-off all Servers after soft shut down procedure Step 3: Shut down main circuit located on the bottom floor Step 4: Use emergency phone line to make outgoing phone calls Step 5: Call power company for assessment Step 6: Locate sources of mobile power Step 7: Contact electrical company Step 8: Re-energize building Step 9: Power-on equipment
Urban Fires	In metropolitan areas, urban fires can, and do, cause hundreds of deaths each year and **Lagos** is no exception. Even with strict building codes and exceptions, citizens still perish needlessly in fires.	Step 1: Attempt to suppress fire in early stages Step 2: Evacuate personnel on alarm, as necessary Step 3: Notify fire department Step 4: Shut off utilities Step 5: Account for all personnel

HAZARD:	PROFILE OF HAZARD:	FIRST RESPONSE:
		Step 6: Search for missing personnel Step 7: Asses damage

2.4 Recovery Strategy Overview

NSE's Business Continuity Recovery is based on the organization surviving the loss of facilities and/or key personnel and systems during a disaster.

Once NSE's ERT has determined that a declaration of disaster is required, the following sequence of events will occur:

STEPS:	INSTRUCTION:
1: Evacuate affected facility.	**If the emergency requires an evacuation of employees, execute evacuation plans contained in the Emergency Procedures section.**
2: Go to staging area.	Follow building evacuation instructions.
3: Determine length of outage.	**Review written and verbal damage assessment reports from facilities and civil authorities and then estimate the amount of time the facility will be uninhabitable.**
4: Select disaster level.	Based on the estimated duration of the outage, declare the disaster event as either a L1 (Less than 48hrs.), L2 (48hrs. to 6 weeks), or L3 (6 weeks or longer).
5: Activate alternate facilities.	**Contact alternate facilities identified in the Facilities section. Confirm their availability and alert them of estimated arrival time.**
6: Release personnel from the staging area.	Once the disaster level has been selected, release all personnel from the staging area to their assigned recovery location. • Non-essential personnel – Home • Recovery Site Team – Alternate Facility • End Users – Alternate Facility • Command Center Staff – Alternate Facility • Crisis Management Team – Alternate Facility
7: RST establish Command Center.	**RST personnel are the first to arrive at the alternate facility to setup and organize the command center prior to the arrival of the CMT and support personnel. The following representatives are required at the Command Center within 1-3 hours:** • **Crisis Management Team** • **Emergency Response Team Lead**

STEPS:	INSTRUCTION:
	• Business Restoration Team Lead • Recovery Site Team Lead
8: Establish situation desk.	At the command center, establish a dedicated line with operator to field all incoming calls. Announce command center phone number to all recovery participants.
9: Review recovery matrix.	Review the Recovery Matrix Section on a department by department basis to determine who is most affected by the disaster. Group departments by recovery resource requirements, time frames, and co-location requirements.
10: Create technology shopping list.	Once the technology requirements of the effected department(s) are known, create a requirements list for the IT support staff.
11: Contact quick ship vendors.	Using the vendor quick-ship contacts or local sources located in the LAN Restoration section order replacement technology indicated on requirements list.
12: Retrieve electronic/hardcopy vital records,	Retrieve vital records from locations as indicated in the Vital Records section. Have vital records shipped and staged at the alternate facility.
13: Setup replacement LAN.	The priority of NSE Server restoration to support all other NSE Business functions is: • Core technology • End-user servers
14: Activate short-term recovery strategies.	Instruct each department to initiate their short-term recovery strategies. These strategies will be used while the replacement LAN/WAN circuits are implemented.
15: Populate alternate facility.	Once the replacement LAN/WAN is functional, notify the BRT that departments can now begin executing their L2 recovery strategies.

2.5 Plan Participants

The following presents the NSE plan participants and their associated recovery function. At the time of a disaster, these individuals will be among the first to be contacted.

RECOVERY ROLE:	PRIMARY:	ALTERNATE:
Recovery Manager	Name: _____	Name: _____

RECOVERY ROLE:	PRIMARY:	ALTERNATE:
	Title: Office: Cell: Home: E-mail: Pager/other:	Title: Office: Cell: Home: E-mail: Pager/other:
Voice Recovery	**Name:** **Title:** **Office:** **Cell:** **Home:** **E-mail:** **Pager/other:**	**Name:** **Title:** **Office:** **Cell:** **Home:** **E-mail:** **Pager/other:**
IT Recovery	Name: Title:	Name: Title:

RECOVERY ROLE:	PRIMARY:	ALTERNATE:
	_____ Office: _____ Cell: _____ Home: _____ E-mail: _____ Pager/other:	_____ Office: _____ Cell: _____ Home: _____ E-mail: _____ Pager/other:
Network Recovery	Name: _____ Title: _____ Office: _____ Cell: _____ Home: _____ E-mail: _____ Pager/other:	Name: _____ Title: _____ Office: _____ Cell: _____ Home: _____ E-mail: _____ Pager/other:
Administrative Support	**Name:** _____ **Title:**	**Name:** _____ **Title:**

RECOVERY ROLE:	PRIMARY:	ALTERNATE:
	Office:	Office:
	Cell:	Cell:
	Home:	Home:
	E-mail:	E-mail:
	Pager/other:	Pager/other:

2.6 Alternate Site Setup

Alternate Site Configuration and Checklists

Once the alternate site has been secured, the RST's will work with the event staff to configure appropriate command enter and recovery space.

The following provides **NSE** configurations for general work areas and the command center.

RECOVERY AREA:	CONFIGURATION:
Command Center	• Occupancy – 15 • Room – private, 750-sq. ft. • Conference table • Phones – 15 • Facsimile – 2 • Office Equipment – copier, PC, printer, folding tables • Office supplies – flip charts, stationary, writing supplies • Communications – Walkie-talkies, tape recorder, cellular phones
Work Area Recovery	• Occupancy – 50 • Room – 5000- sq. ft. • Folding Tables- each workstation needs to be 3ft apart • Phones – 50

RECOVERY AREA:	CONFIGURATION:
	• Facsimile – 3 • Office Equipment – copier, recorder, 15 pre-configured laptops • Office supplies – flip charts, stationary, writing supplies • Communications – 3 fax lines, 10 modem lines, 50 voice lines
Mail Room	• Occupancy – 2 • Room – 250-sq.ft. • Phone – 1 • Office Equipment – scale, postage meter • Supplies – Mailing/shipping supplies
Vital Records Staging	• Occupancy – 2 • Room – private, 300 sq. ft. • Office Equipment – folding tables, metal racks

3.0 Recovery Ranking

The following organization processes will be recovered within the sequence specified below:

PRIORITY RANK:	ORGANIZATION PROCESS:	POTENTIAL IMPACT:	ALLOWABLE DOWNTIME:
1			
2			
3			
4			
5			

PRIORITY RANK:	ORGANIZATION PROCESS:	POTENTIAL IMPACT:	ALLOWABLE DOWNTIME:
7			
8			
9			
10			

4.0 Recovery Team Checklists

Develop checklist for each recovery function:

RECOVERY FUNCTION:	ADMINISTRATION	PRIMARY:	JANE DOE
		ALTERNATE:	JOHN DOE
ALTERNATE LOCATIONS:	Primary Staging Area:		Alternate Staging Area:
	Primary Work Area:		Alternate Work Area:
CHARTER:	Responsible for all of the administrative aspects of the recovery effort. This includes maintaining the plan currency, activating the command center and providing logistics and employee assistance support during the recovery effort.		
RETRIEVAL LIST:	The following items should be removed from your work area if you are evacuated from the building: 1.		

RECOVERY FUNCTION:	**ADMINISTRATION**	**PRIMARY:**	**JANE DOE**
		ALTERNATE:	**JOHN DOE**
	2. _____ **3.** _____ **4.** _____ **5.** _____ **6.** _____		
RECOVERY RESOURCES:	**In order to perform your recovery efforts, you will need access to the following resources:**		
	Phone: _____	**PC:** _____	**Network** _____
	Internet _____	**Fax** _____	
RECOVERY STEPS:	**The following are the recovery tasks to be followed:** **1. Retrieve important items form work area** **2. Evacuate building** **3. Go to primary staging area** **4. Wait for all clear or activation notice** **5. Go to designated recovery location** **6. Execute calling tree** **7.** _____ **8.** _____ **9.** _____ **10.**		

RECOVERY FUNCTION:	ADMINISTRATION	PRIMARY:	JANE DOE
		ALTERNATE:	JOHN DOE
	11. _____ 12. _____ 13. _____ 14. _____ 15. _____ 16. _____ 17. _____ 18. _____ 19. _____ 20.		
VITAL RECORDS:	The following documents and/or electronic media will be required for your recovery effort:		

RECOVERY FUNCTION:	ADMINISTRATION	PRIMARY:	JANE DOE
		ALTERNATE:	JOHN DOE
	1. _____ 2. _____ 3. _____ 4. _____ 5. _____		

5.0 Emergency Contacts

5.1 Vendor Dependencies

All plans require a comprehensive listing of external contacts:

PROVIDER:	CONTACT:	PURPOSE:
(Name)	(Phone / Email)	Power protection systems
		Mobile recovery resources
		Electronics restorations
		Damage restoration (fire & water)
		Crisis management
		Online data backup
		Data restoration services
		Disaster response kits
		Expedited shipping
		Emergency power supply

PROVIDER:	CONTACT:	PURPOSE:
		Crisis management
		Off-site data storage
		Diesel generators.
		Mail processing recovery
		Damaged media recovery
		Satellite linked command center
		Data recovery and forensics
		Emergency technology recovery
		Fire, smoke & water restoration
		Cleanup and restoration services
		Hot sites, warm sites, and cold sites

6.0 Emergency Procedures

This section is reserved for specialized emergency procedures.

APPENDIX 13

13. Sample Mumbai DRP

Disaster Recovery Plan of the National Stock Exchange

Mumbai

Table of Contents

1. Sector
2. Sub-sector
3. Area

13. Knowledge Management
    13.1. Models/ Refinements conceived and implemented
14. Unfolding Story
    14.1. Overview of genesis
    14.2. Synopsis of development that led to design of initiative
15. Impact
16. Feedback for continuous improvement
17. Policy Support
18. Change Management Strategy
    18.1. Approach
19. Deployment Model
    19.1. Strategy for deployment
20. Business Model
    20.1. Description
    20.2. Factors critical to sustainability
21. Leadership
    21.1. Key factors which led to success/failure
    21.2. Impediments, if any
22. Standard Operation Procedures
23. Cost
24. Artifacts
25. Glossary of Stock Exchange Terms used
26. Key implementing agencies

Table of Artifact

Figures

Figure 1: Map showing Stock Exchanges in India

Figure 2: The 5 companies of NSE Group

Figure 3: NSE Model

Figure 4: Overview of NSE IT Setup

Figure 5: Corporate Network

Figure 6: NSE Data Communication through VSATs

Figure 7: NSE System Architecture

Figure 8: The orbiting satellite INSAT 3B

Figure 9: Satellite Communication System Frequency

Figure 10: BCP Essentials

Figure 11: NSE BCP & DR Model

Figure 12: DR strategy ranges

Photos

Photo 1: NSE Mumbai

1. Sector

   Services

2. Sub-sector

   Financial Services

3. Area

   Disaster Recovery & Business Continuity Planning

4. Project

   4.1. Title

   Disaster Recovery Plan of the National Stock Exchange Limited, Mumbai

   Description

   The Business Continuity Management Plan and an elaborate Disaster Recovery (DR) site at Chennai ensure continuity of normal critical trade and settlement operations of NSE, even during a disaster.

5. Case Study

   5.1. *Title*

   Disaster Recovery Plan of the National Stock Exchange

   Description

   The National Stock Exchange (NSE) is one of the largest exchanges in India and uses over 3,000 VSAT links, owns two VSAT hubs, and is linked to around 1,000 leased lines. Each VSAT link connects to multiple traders in 360 cities nationwide. The systems support around 7,000 concurrent users daily.

   NSE needed to set up a Disaster Recovery (DR) infrastructure to:

   - Attract international investors
   - Offer Business Continuity (BC) during a disaster
   - Follow BC policies

   NSE set up a live DR site in Chennai. Data from the critical business applications are replicated at the site.
   All critical daily operations at NSE can continue during a disaster. The live DR site can immediately take over in case of a disastrous event.

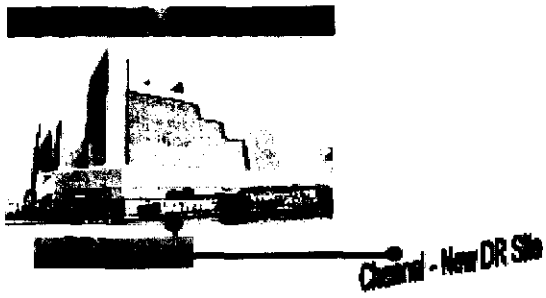


Photo 1: NSE Mumbai

5.2. Key words

Business Continuity Plan (BCP)/Disaster Recovery (DR) –

Process of developing advanced arrangements and procedures that help an organization respond to an event in such a manner that critical business functions continue without interruption or significant change.

6. Executive Summary

The idea of planning to meet a disaster situation is not new. As early as in fifties, GOI used to insist on preparing civil defense measures in the event of a disaster, especially in river valley projects. Till recently, ICT-intensive companies were paying lip service to the idea of a BCP/DR. Increased threat of attacks like power outages, fires, floods and terrorism (9/11 WTC Disaster) coupled with regulations stipulated by regulatory bodies to ICT-dependent businesses and international competition have all made these businesses to seriously plan and implement/maintain BCP/DR.

The National Stock Exchange of India Limited is a pioneer in planning and maintaining a secondary DR site at Chennai so that its operations can continue in the event a disaster strikes.

The NSE primary site at Mumbai can rightfully boast of having one of the world's largest ICT infrastructures with mainframe computers, large servers, thousands of PCs and a VSAT communication system covering about 400 cities and towns in India. How much of this infrastructure should be replicated at the DR site at Chennai so that the mission-critical operations of NSE can be continued within the shortest time after the disaster strikes? This was the major challenge.

The strategy included business impact analysis; DR strategy selection; and BC planning, maintaining and testing. Major infrastructure at the primary site required for mission-critical operations of NSE during a disaster have been replicated at the DR site.

The DR site has been planned and executed by NSE IT Limited, a subsidiary of NSE responsible for ICT. A dedicated core team comprising both business and IT staff, is responsible for the entire BCP operations. The function of this group is to ensure successful drills, update the checklist for BCP operations on a continuous basis and maintain exhaustive documentation on the BCP procedures, which includes details of

classification of events falling under disaster category, and the *corresponding action* plan.

In the event of an actual disaster, a nominated commander of the BCP team would assume charge and control operations from a pre-*allotted command room*.

Systems have been designed to switch over in such a way that NSE would be online again the very next day. But if a disaster occurs at the beginning of the day (before the market opens), *NSE could be online in an hour's time (by switching* to the backup systems at the primary site itself). The DR site costed about Rs. 40 crore.

NSE.IT has gained a lot of expertise and knowledge about BCM from all the projects *that its team has implemented for NSE. NSE.IT now hopes* to pass on this wisdom to other organizations by way of offering consultancy and planning services.

7. Contributors and References

7.1. Key Architects

National Stock Exchange Limited (Mr. Ravi Narain, MD & CEO, Mr. G M Shenoy, Vice-president of Information Technology)

NSE.IT Limited (Mr. Satish Naralkar, CEO; Mr. C. Kajwadkar, Vice-President)

7.2. *Implementers/ Stakeholders*

National Stock Exchange Limited
NSE.IT Limited

7.3. Documenting Authors

Mr. Satish Naralkar, CEO NSE IT Limited
Mr. C. Kajwadkar, Vice-President NSE.IT Limited
Mr. Soutiman Das Gupta (soutimand@networkmagazineindia.com) and Mr. Brian Pereira (brianp@networkmagazineindia.com) have reported/interviewed on the case.

7.4. Sources/ References

1. http://www.networkmagazineindia.com/200304/case1.shtml
2. http://www.networkmagazineindia.com/200208/cover2.shtml
3. http://www.expresscomputeronline.com/20030602/indtrend1.shtml
4. http://www.hcasia.com/ViewArt.cfm?Magid=3&Artid=21978&Catid=2&subcat=44
5. http://www.nseindia.com/
6. http://encyclopedia.thefreedictionary.com/National%20Stock%20Exchange%20India
7. http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,92988,00.html
8. http://www.nse-india.com/
9. http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,92265,00.html
10. http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,91587/p2,00.html
11. http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,91952,00.html
12. http://www.webopedia.com/TERM/V/VSAT.html
13. http://www.asx.com.au/webmcq/servlet/com.webmcq.glossary.Glossary?oid=0&alt=1#anchor0

14. http://www.nasscom.org/artdisplay.asp?Art_id=1856
15. http://www.networkmagazineindia.com/200211/nse.shtml
16. http://www.ncasia.com/ViewArt.cfm?Magid=3&Artid=21978&Catid=2&subcat=44
17. http://www.expresscomputeronline.com/20030602/indtrend1.shtml
18. http://www.networkmagazineindia.com/200305/inperson.shtml
19. http://www.thehindubusinessline.com/iw/2004/06/27/stories/2004062700940600.htm
20. http://www.networkmagazineindia.com/200304/20030408cov1.jpg
21. http://www.intech.unu.edu/research/past-research/Earlier%20projects/teleworking-india-444/qualititive-financial-summary.pdf
22. http://www.gilat.com/Technology_SatelliteBasics.asp
23. http://www.wtec.org/loyola/satcom2/f_02.htm
24. http://www.gilat.com/Technology_SatelliteBasics.asp
25. http://asia.spaceref.com/news/viewpr.html?pid=1226
26. http://www.frontierstatus.com/fs0195.shtml
27. http://www.networkmagazineindia.com/200206/case1.shtml
28. http://www.networkmagazineindia.com/events/is2003/kajwadkar.pdf
29. http://www.expresscomputeronline.com/20020826/storage7.shtml
30. http://www.expresscomputeronline.com/20020826/storage6.shtml
31. http://www.investopedia.com/categories/tradingterms.asp
32. http://www.channeltimes.com/channeltimes/jsp/banneradmin/redirect.jsp?ad_id=1360&page=http%3A%2F%2Fwww.cxotoday.com%2Fcxo%2Fjsp%2Freqstep1.jsp
33. http://www.cxotoday.com/cxo/jsp/showstory.jsp?storyid=547
34. http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/x25.htm#xtocid2
35. http://www.nseindia.com/content/us/fact2001_sec1.pdf

8. Organization

8.1. Name of the Organization

The **National Stock Exchange India, Limited**

8.2. Head of the Organization

Chairman of the Board of Directors

8.3. Location

Location

The National Stock Exchange India is located in Mumbai City (Maharashtra State), the financial capital of India.

- *Establishing a nation-wide trading facility for equities, debt instruments and hybrids,*
- *Ensuring equal access to investors all over the country through an appropriate communication network,*
- *Providing a fair, efficient and transparent securities market to investors using electronic trading systems,*
- *Enabling shorter settlement cycles and book entry settlements systems, and*
- *Meeting the current international standards of securities markets.*

The standards set by NSE in terms of market practices and technology have become industry benchmarks.

Market segments:

☐ Capital Market (Equities) (CM)	☐ Futures & Options (Derivatives) (F&O)
☐ Wholesale Debt Market (WDM)	☐ Initial Public Offer (IPO)
☐ Mutual Funds (MF)	

NSE's market share is 64% in CM and 99% in Derivatives.

Refer Figure 2.

NSCCL National Securities Clearing Corporation Limited - Settlement of claims related to equities, securities

NSDL National Securities Depository Limited - Dematerialization of Securities

IISL India Index Services and Products Limited - Index related Services and Products

DotEx Intl Ltd - DotEx International Limited - Internet Trading Platform

NSE.IT NSE.IT - Limited Information - Techno Arm of NSE

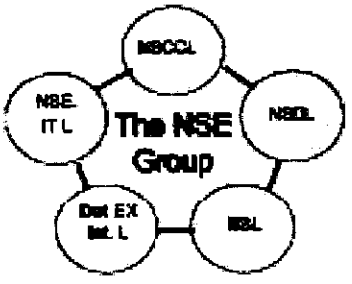


Figure 2: The 5 companies of NSE Group

8.4. Structure

NSE is one of the first **de-mutualised** stock exchanges in the country, where the ownership and management of the Exchange are completely divorced from the right to trade on it.

NSE is a public limited company **owned** by a set of leading financial institutions, banks, insurance companies and other financial intermediaries in the country.

Professionals, who do not directly or indirectly trade on the Exchange, **manage** it.

The NSE model however, does not preclude, but in fact accommodates involvement, support and contribution of trading members in a variety of ways.

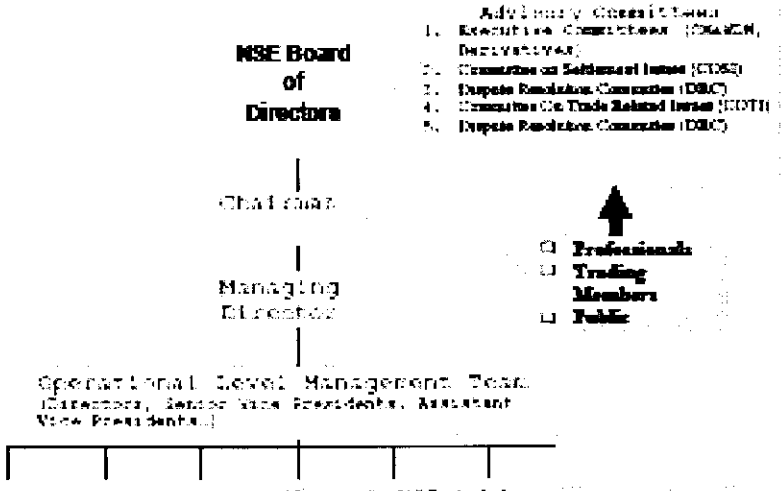


Figure 3: NSE Model

NSE has launched many indices for the exchange like S&P CNX Nifty and CNX Nifty Junior.

NSE has brought about transparency, speed & efficiency, safety and market integrity. It has set up facilities that serve as a model for the securities industry in terms of systems, practices and procedures.

It uses state-of-art information technology to provide an efficient and transparent trading, clearing and settlement mechanism.

Its average daily turnover is Rs 8,000-9,000 crore.

Key IT Infrastructure at the Primary Site

NSE's IT set-up is the largest by any company in India. In order to capitalize on in-house expertise in technology, NSE set up a separate company, NSE.IT, in October 1999. Figure 4 is an overview of IT setup in NSE.

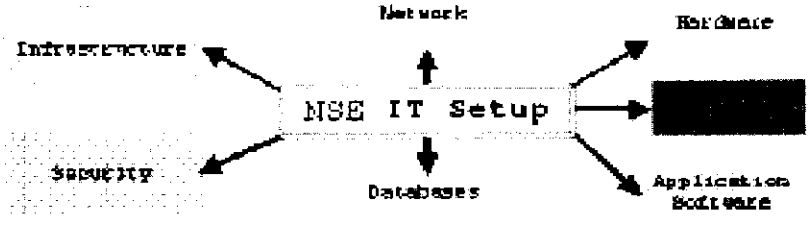


Figure 4: Overview of NSE IT Setup

Hardware	
Description	**Number**
Stratus Mainframe (Fault Tolerant System)	11
Digital Alpha (Large Unix Servers)	6

HP 9000 (Large Unix Servers)	4
Digital Alpha/Sun (Medium Unix Servers) Compaq/HP/Dell (NT / 2000 Servers)	15 55
Workstations	1068
Software	
OS	VOS/UNIX (Digital/HP/SUN) WINDOWS NT/ WINDOWS 2000
Database	Oracle, MS SQL, RAIMA, Appletree
Front End	Windows NT/2000/XP, Developer 2000, CTD, Visual C++
Tools	Oracle Case Tool, Designer 2000, SQL Back Track, Veritas Backup/Restore Network Monitoring (VSAT & Terrestrial Based Trading Network-TBTN)
GroupWare	Lotus Notes
Communication Protocols	X-25, TCP/IP

The trading server software runs on a fault tolerant STRATUS main frame computer. The client software runs under Windows on PCs.

NSE uses powerful RISC -based UNIX servers. It currently manages its *data centre operations, system and database administration, design and development of in-house systems* and *design and implementation of telecommunication solutions. NSE has also* put in place NIBIS (NSE's Internet Based Information System) for on-line real-time dissemination of trading information over the Internet.

The original implementation for the equities market used a traditional RDBMS/mainframe approach. Currently LINUX (RedHat Linux 7.2) and parallelism are used for the derivatives segment. The system NSE set up for doing VaR (Value at Risk) calculations is Prism (Parallel RISk Management system) software deployed on an Intel *Xeon server and seven PC's all based on RedHat Linux 7.2.*

Data Networking

The National Stock Exchange is the second stock exchange in the world, after NASDAQ, to implement a Data Warehouse. NEAT (National Exchange for Automated Trading) is a state-of-the-art client server based application. At the server end, all trading information is stored in an in-memory database to achieve minimum response time and maximum system availability for users. Network elements like storage, security, backup and recovery processes, availability, and the different applications are carefully planned and commissioned, following stringent RBI regulations to store at least 7 years of transactional and financial data.

Considering high volumes of data that NSE is handling, it has deployed network-based storage SAN.

Telecommunication Network

NSE uses satellite communication technology through VSATs to energize participation from around 400 cities spread all over the country. NSE can handle up to 1 million trades per day.

The telecommunications network uses X.25 protocol (an International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) protocol standard for WAN communications that defines how connections between user devices and network devices are established and maintained). It is the backbone of the automated trading system. Each trading member trades on the NSE with other members through a PC located in the trading member's office, anywhere in India.

The trading members on the Wholesale Debt Market segment are linked to the central computer at the NSE through dedicated 64Kbps leased lines and VSAT terminals. These leased lines are multiplexed using dedicated 2 MBPS, optical-fibre links. The WDM participants connect to the trading system through dial-up links.

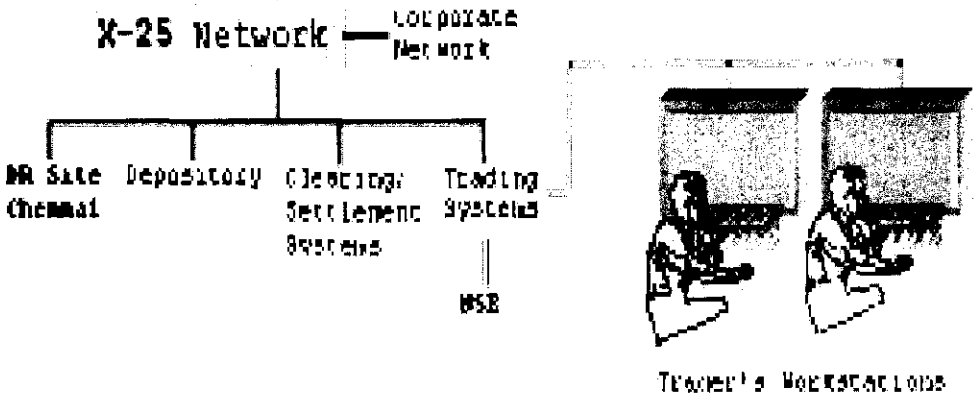


Figure 5: Corporate Network

NSE is one of the largest interactive VSAT-based stock exchanges in the world. Today it supports 3000 VSATs and is expected to grow to more than 4000 VSATs. *The NSE-network is the largest private wide area network in the country and the first extended C- Band VSAT network in the world.* Currently more than 9000 users are trading on the real time-online NSE application.

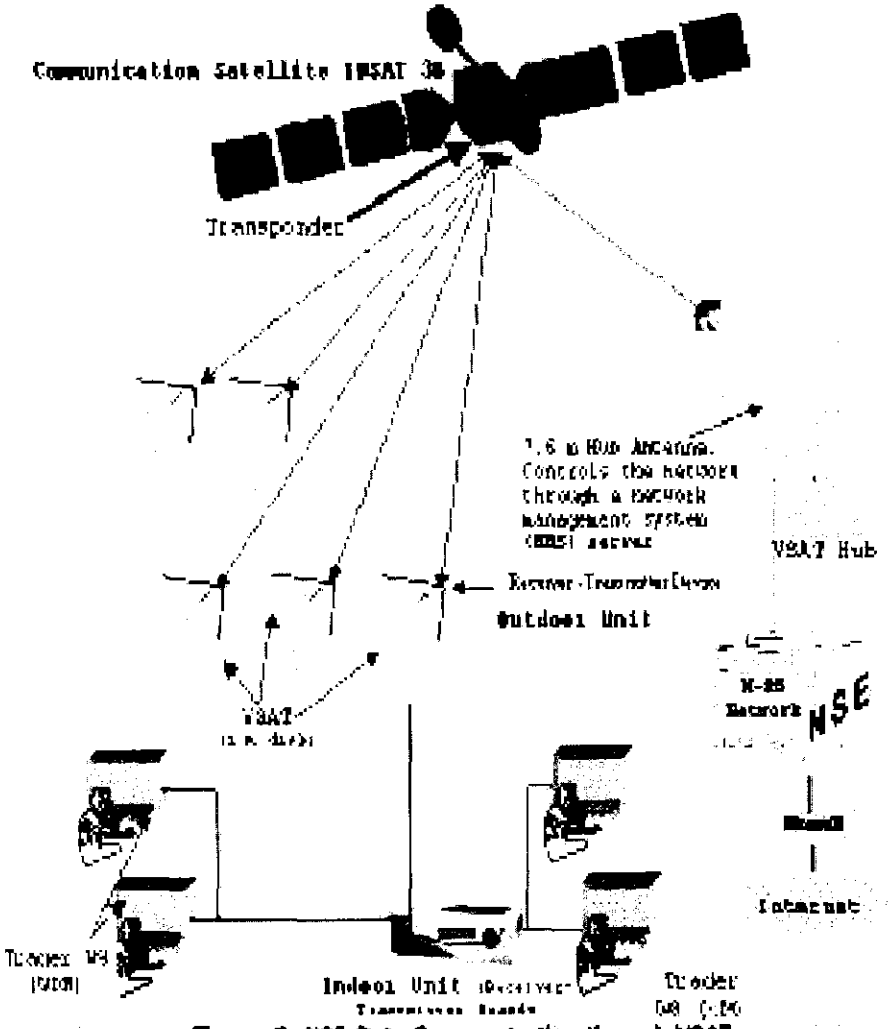


Figure 6: NSE Data Communication through VSATs

The following companies have provided technical services shown against each.

- HCL Comnet Systems and Services Ltd. (VSAT Services)
- Wipro Technologies Limited (Data Warehouse)
- TCS Limited (Software)

The detailed system architecture is presented in Figure 7.

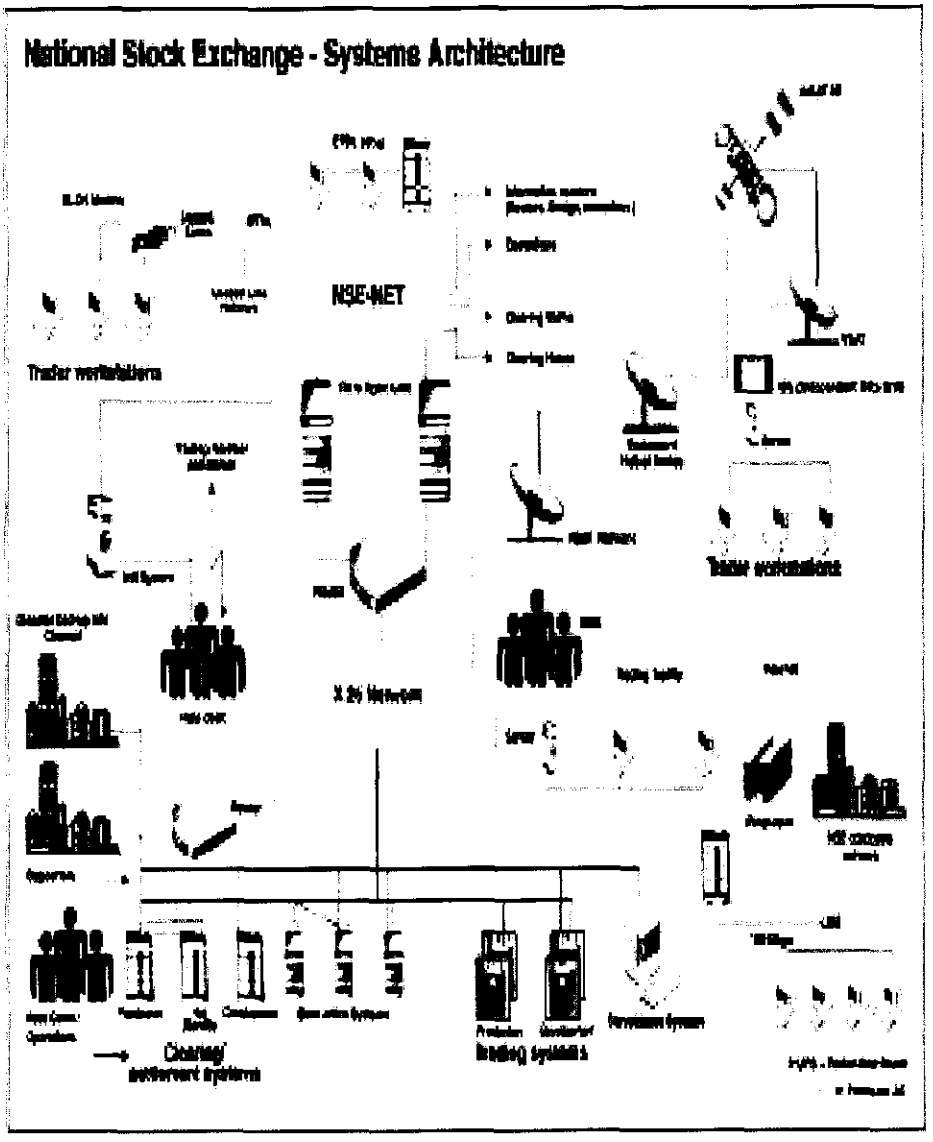


Figure 7: NSE System Architecture

The VSAT (Very Small Aperture Terminal) System

VSAT system is a private satellite network for communicating data, voice and video signals (excluding broadcast television) useful to organizations with activities dispersed *over large areas. A VSAT consists of 2 parts, a transmitter* that is placed outdoors in direct line of sight to the satellite and a receiver that is placed indoors to interface the transceiver with *the end user's communications device, such as a PC.* The transceiver receives/ sends a signal to satellite transponder in the sky. The satellite sends/ receives signals from a ground station computer that acts as a hub for the system. Each end user is interconnected with the hub via the satellite, *forming a star network.* The hub controls the entire operation of the network. For one end user to communicate with another, each transmission has to first go to the hub station that then retransmits it via the satellite to the other end user's VSAT.

1. **View "Discover Satellites" in http://www.gilat.com/GilatWorldwide.asp to understand the working of VSAT.**
2. **Click "Meet the VSAT" to interact with a VSAT to know its parts in http://www.gilat.com/Technology_SatelliteBasics.asp**

A corporate *network* has been implemented, connecting all the offices at Mumbai, Delhi, Calcutta and Chennai.

Currently, NSE is displaying its live stock quotes on the web site (www.nseindia.com) which are *updated online.*

Communication Satellite INSAT 3B

A satellite is a specialized wireless receiver/transmitter - essentially a radio-frequency repeater - that is launched by a rocket and placed in orbit around the earth. A single transponder on one of these satellites (the part of the satellite that transmits signals back to Earth, of which a typical satellite has 32) is capable of handling approximately 100 million bits of information per second. This means that if the transponder is accessed for only 90 seconds per day, close to a billion bytes of data would be transferred - the equivalent of 865 000 double-spaced pages. With this immense capacity, today's communication satellites are an ideal medium for transmitting and receiving almost any kind of content, from simple data to the most complex and bandwidth-intensive video, audio and data content.

INSAT 3B is a $110 million ISRO communication satellite which has given a great impetus to VSAT technology in India.

Figure 8: The orbiting satellite INSAT 3B

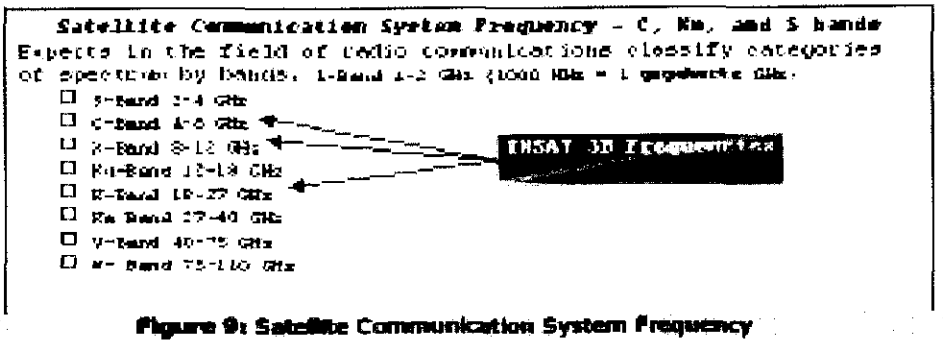


Figure 9: Satellite Communication System Frequency

Project Design

Key Objectives

To ensure uninterrupted service by NSE through adequate measures to support business recovery, which includes a DR site in another city. The goal is primarily BCM. In the case of the severest damages, NSE should be up and running within the shortest possible time. The DR plans are continuously updated and in the event of a disaster, NSE can be back in business within 24 hours.

Outcomes

NSE deployed a basic BCM program in 1997 at its primary site in Bandra-Kurla Complex, Mumbai. It comprised redundant systems with adequate backup and failover. The BCM infrastructure was further developed and in 1998, NSE set up its first DR site in Pune. The DR site was migrated to Chennai in 2002. **This has made NSE the only exchange in India with a live DR site.**

Time taken to switch to the DR site

Systems have been designed to switch over in such a way that NSE would be online again the very next day. But if a disaster occurs at the beginning of the day (before the market opens), NSE could be online in an hour's time (by switching to the backup systems at the primary site itself).

Strategy - BCP essentials are shown in Figure 10.

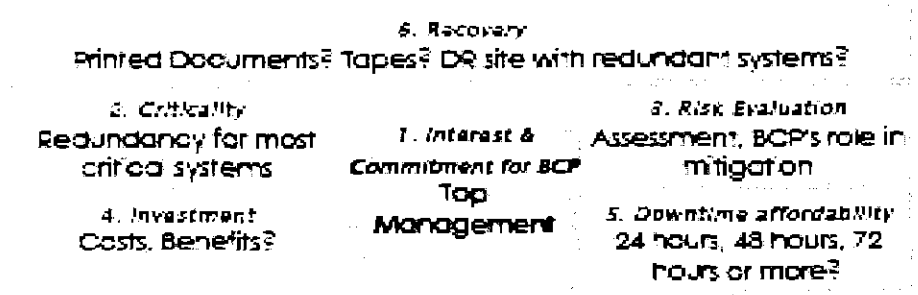


Figure 10: BCP Essentials

NSE management identified a minimum number of critical business processes and resources to maintain an acceptable level of business in the event of a disaster.

NSE had to ensure that the requirements of online and real-time data could be restored as quickly as possible.

A detailed business impact analysis was prepared, which weighed the impact of specific disasters against key business processes. Apart from the site being located in a different city, it had to also be easily linked to the main site via high-speed links, for online real-time connectivity.

Also, while the company had the option of cutting down costs by installing only the minimum required infrastructure at the backup site, no compromises were made, and the entire infrastructure was replicated. However, processes, which were not crucial for the day-to-day functioning of the company, were excluded.

NSE achieved its BCP and DR goals by planning which comprised the main building blocks shown in Figure 11.

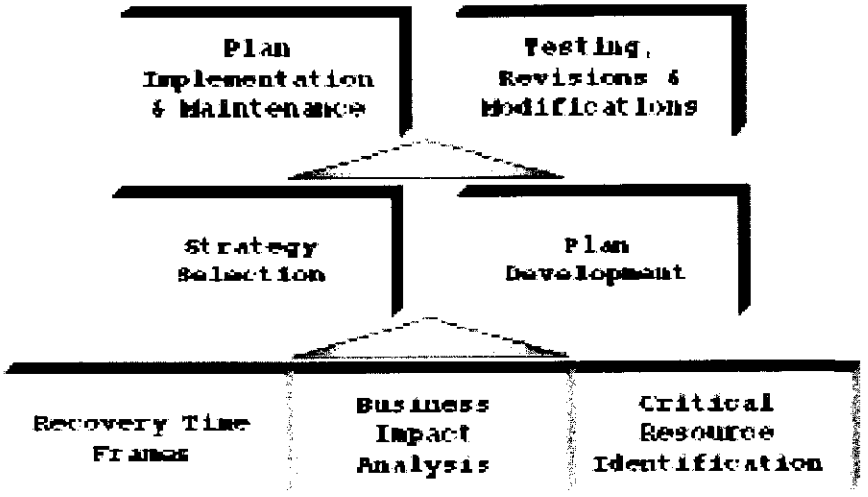


Figure 11: NSE BCP & DR Model

Brief description of key activities

a. **Business Impact Analysis**
This studied the impact, in case business fails to run. This was necessary to justify any investment in BC and DR infrastructure. Collective wisdom from NSE's business and operation heads was sought. The critical applications pertinent to the business were defined and covered in the DR infrastructure. A DR solution is a perpetual effort. What is done at the primary site must be replicated at the DR site.

b. **Selection of Strategy**
BC strategy requirements were identified. Business, technology, and non-technology recovery issues were looked into and aspects like timeframes, options, locations, personnel, and communications were provisioned.

Figure 12 shows a range of DR solutions depending on importance of data, amount of data and recovery time. For example, if the recovery time is *immediate* and the importance and amount of data is *more* then a *completely duplicated interconnected hot site* is the solution.

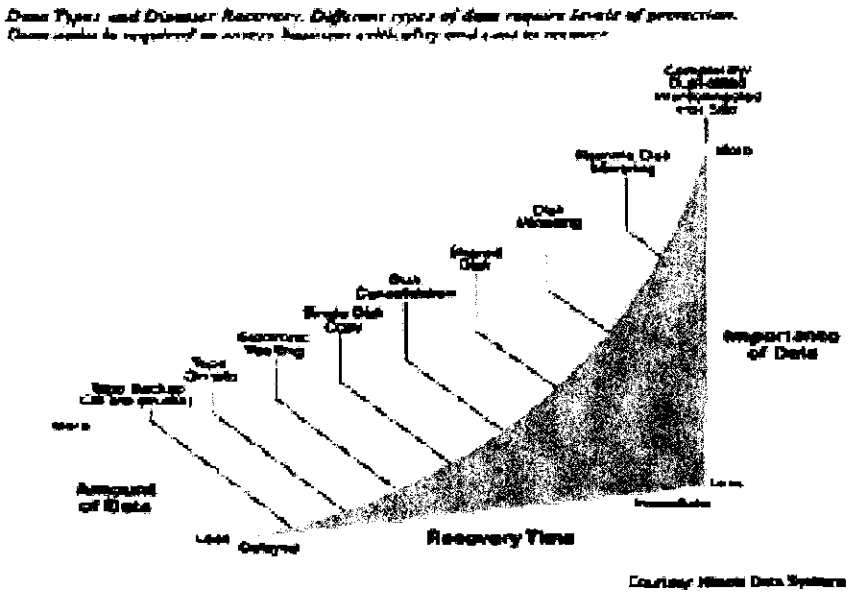


Figure 12: DR strategy ranges

The total volume of data residing in NSE's systems runs into 2-3 terabytes, and is expected to grow to 7.5 terabytes over the next four years. Any downtime is unacceptable at NSE since the business lost due to data loss can be tremendous.

An alternative recovery strategy and the risk associated with each strategy were made. A cost benefit analysis of recovery strategies and present findings were presented to the senior management. Alternate storage sites were identified. Provisions were made for emergency telecommunications and data communication.

c. **Detailed Plan Development and Maintenance-This involved defining**
   - *Plan development requirements (job descriptions, action plans, checklists, matrices and flowcharts).*
   - *Recovery management and control requirements like team description and team organization.*
   - *Plan components, drafts, and BC procedures.*
   - *IT recovery procedures.*

d. **Testing, Revisions and Modifications-This step included**
   - *Establishing an exercise program, defining exercise requirements, developing realistic scenarios, and creating schedules.*
   - *Post exercise reporting.*
   - *Establishing review criteria.*
   - *Setting audit objectives and scope.*
   - *Reviewing policies periodically or after events.*

Different types of DR methods

1. Backup to tape periodically and shipping the tapes to a remote DR location or storing them in a fire-proof/earthquake-proof safe vault.
2. Replicate data from servers in the data centre to servers in the remote location.
3. Replicate data from storage in data centre to storage in the remote location.

Annex 1 presents the best practice for BCP & DR.
Annex 2 presents a practical case of DR.

Risk Perception

The **biggest risk to business continuity** is the lack of conviction among the top executives of the enterprise that a risk actually exists. Enterprises have to be proactive in formulating and maintaining Business Continuity Management Plan more seriously and not wait for disaster to strike first.

For instance, NSE's IT infrastructure includes multiple fault tolerant mainframe computers, dozens of UNIX and NT servers and more than a thousand PCs. NSE is also one of the largest interactive VSAT-based stock exchanges in the world, supporting more than 3,000 VSATs over 400 cities. Without a DR plan, in case a disaster were to strike NSE's primary site at Bandra-Kurla Complex damaging the entire set up, it would take a minimum of four months to re-establish the network. Imagine the direct business loss 4 x 20 x 8000 = Rs. 6,40,000 crore!

Business loss in case of a disaster

There are a nearly a million transactions routed through NSE daily. The mission-critical applications at NSE include trading, clearing and settlement, surveillance, position monitoring and risk management. During trading hours, there are about 7,000 participants logged on to the system. The daily turnover at NSE from its three market segments aggregates to over Rs 8,000 crore. In case disasters strike in the form of an earthquake, or say a terrorist attack, the impact would be catastrophic.

But most importantly, the loss of trading hours would not only result in huge tangible and intangible losses, but could also result in permanent closure of the business.

Findings of studies on BCP

As per a study conducted by the University of Texas, 43 percent of companies that experience a disaster, but have no BCP in place ever reopen. The research also states that only one in ten companies that have experienced a disaster, but have no tested BCP in place, are still in business two years later. While other organizations can at least have some moments of respite, as most of the data is not real-time.

Research shows that nearly half the companies that lose their data because of a disaster never re-open and 90 percent are out of business within two years. Gartner estimates that two out of five enterprises that experience a disaster go out of business within five years. Nearly 13 percent of disasters are caused by unplanned outages like fire, power failure or flood, whereas 87 percent are planned outages.

Critical information systems become unavailable due to various forms of attack. Ernest & Young's Information Security Survey 2002 reveals that

- Around 76 percent of the respondents experienced unexpected unavailability.
- Despite this, only 47 percent of Indian companies (as compared to 53 percent globally) have a Business Continuity Plan.
- Over half the respondents do not have agreed recovery timescales. *which could mean wide expectation gaps in the event of business interruption.*

The two main causes of unavailability of systems cited by Indian companies, were:

- Malicious technical acts by outsiders (26 percent)
- Third-party failure (14 percent).

Only 17 percent of the respondents said that invoking the BCP/DRP had been effectively done. However only 12 percent of the respondents have tested their plans in the past three months.

In NSE, even a single minute of failure in trading operations could result in a huge loss.

Analyzing Impact

In case of a disaster the tangible and intangible losses will be tremendous.

- Loss due to impact on daily turnover-based revenue in WDM, CM, and derivatives (Rs.8000 crore +).
- Loss of brokerage on daily trading (Average 0.5%).
- Loss of earnings of NSE's business partners like clearing corporations, depositories, and clearing banks.
- *Loss due to legal liabilities that may arise.*
- Loss of trading opportunity to the trading members.
- Loss of image for NSE, the Indian securities industry, and the nation at large.
- *Loss in customer base and goodwill.*

The lack of a BCM plan and DR infrastructure will result in unpredictable recovery time and chaotic recovery of operations.

Project timeframes

NSE had formulated a comprehensive disaster recovery plan as early as 1996 just two years after it commenced operations when the BCP concept was unknown in Indian IT circles.

In 1997, NSE leased premises in Pune and began to build its first DR site. It went live in 1998. Pune was chosen mainly because it was geographically near Mumbai, making it easy to move staff between the primary site and the DR site. NSE maintained skeleton staff at this facility.

Live drills were performed from Pune, where critical applications were entirely run from the DR infrastructure. Essential staff was shifted from Mumbai prior to the drill.

In 2001, the DR site was migrated to Chennai. The new site was operational in mid-2002.

Key Implementing Agencies

a. The National Stock Exchange of India Ltd.

b. NSE.IT Limited which implements all IT -related projects at NSE.
NSE.IT, a 100% subsidiary of NSE, has over 800 companies listed and has a daily *trading volume of Rs. 2,472 Crore. NSE.IT* is uniquely positioned to provide products, services and solutions for the securities industry. NSEIT, a profit centre of NSE group, provides systems and telecommunication services to NSE besides independently generating and marketing software (Neat XS™, Neat IXS™, ProBos™, Endorsor™, Enlibor™, PRISM) for market intermediaries.

Neat XS™ is a computer-to-computer link *order routing system*. Neat IXS™ is an *Internet trading system*. It is the first stock exchange to export software.

PRISM
With the introduction of futures and options in portfolio management, PRISM was developed to address the problem of handling real-time risk. PRISM includes a netting engine, customizable risk computing algorithm and other features. NSE required an online system capable of handling up to three times its current volumes (6000 Trades/Minute). In line with *international practices, NSE chose to* use a portfolio based Value at Risk (VaR) model to measure risk.

PRISM includes a netting engine, customizable risk computing algorithm and other features. NSE required an online system capable of handling up to three times its current volumes (6000 Trades/Minute). In line with international practices, NSE chose to use a portfolio based Value at Risk (VaR) model to measure risk.

Performance tests conducted at the super computing facility of the Center for *Development of Advanced Computing have shown that the system* is capable of handling more than 1000 VaR/Second (30,000 Trades/Minute) on the ParamNET architecture. Benchmark tests performed at NSEIL showed that the system handles over 1000 VaR/Second (30,000 Trades/Minute) on a fast Ethernet.

Knowledge Management

Models/ Refinements conceived and implemented

NSE.IT has also been continuously upgrading the BCP documents according to the changes followed at the live site. For example, the BCP plan has changed over 50 percent since the time it was drafted.

Unfolding Story

Overview of genesis

Though IT departments have always been addressing Business Continuity (BC) and Disaster Recovery (DR), some recent developments had a tremendous impact on IT companies/ departments to seriously consider formulating and maintaining the business continuity management plan and DR.

a. WTC disaster on 9/11
b. The threat of an Indo-Pak nuclear war after Kargil Confrontation, Earthquakes, Terrorist Attacks
c. International businesses looking to outsource operations in India will look for companies having a documented Business Continuity Plan (BCP)

d. Companies in India are embarking on DR initiatives to gain an edge over competitors. More and more Indian firms are now operating in a 24x7 environment, especially large enterprises, where global operations are the norm.

The Reserve Bank of India (RBI) has imposed BCP for all banks and Securities & Exchange Board of India (SEBI) has introduced guidelines on BCP for mutual funds companies. Many IT companies will go in for BCP/DR as their overseas clients insist on it.

Other companies which have gone for DR - Examples

GE's BPO Division (India), ONGC, BPCL, Citibank, ICICI Bank, HDFC Bank, Reserve Bank of India, UTI, NIIT, Cisco, SmithKline Beecham, Alstom Power

Synopsis of development that led to design of initiative

Participation of Foreign Institutional Investors (FIIs) in the Indian stock market is important to promote economic reforms in the country. This demands that Indian exchanges follow the practices and guidelines of international exchanges.

In order to maintain international standards and be committed to continuity, NSE has set up and manages its own *DR site in Chennai*. All the critical applications and hardware are replicated at the site, which works as a failover in case of an untoward event at the primary site.

Developments in USA

The U.S. Securities and Exchange Commission has approved rules that require firms to submit business continuity plans detailing how they will provide ongoing access to systems during an emergency. A combination of "peer pressure and regulatory pressure" is prodding companies to ensure that their systems will keep running if a disaster occurs.

Large financial services firms also face an April 2006 deadline for meeting new fed guidelines on increased resiliency for trade clearance and settlement activities.

Impact

In the case of NSE, initially the loss of face to face meetings and personal contacts were perceived to be a disadvantage by the brokers. However, with experience they have come to believe that even in the screen based trading where the brokers do not see each other physically, people are doing much more business than when they were doing in physical form. Technology has been able to overcome the perceived disadvantages in this environment.

A mock, i.e. dummy trading followed internal tests. The DR site went live at the end of March 2002. The primary site at Mumbai was shut down for about two hours, and did live trading was done from the backup site.

NSE has conducted a number of live drills where daily operations at the exchange were conducted entirely out of the DR site. In each drill the performance levels were very satisfactory and the changeover was transparent to the nationwide users.

BCP for a stock exchange is very extensive. Even if the building goes up in flames, it

will be able to continue its operations. The National Stock Exchange is one institution with this capability.

Testing Effectiveness of DR - NASDAQ Experience

NASDAQ announced that it had run tests at its two data centers to check the disaster recovery capabilities of member companies. The tests involved more than 50 brokerages and were conducted at the exchange's primary data center in Connecticut and at its backup facility in Maryland. There was no system downtime at NASDAQ or the participating firms during the tests.

NSE's DR site has certainly improved its credibility in the eyes of the investors and all other stakeholders.

Feedback for continuous improvement

While reviewing the BCP plan, the company observed that since Pune was in the same seismic zone as Mumbai, an earthquake at Mumbai would mean that the Pune site could also be affected. It then took a decision to move the entire infrastructure from Pune to Chennai.

In future, NSE plans to enhance the BCM and DR policies, and follow them. As the primary site adds services, the DR site's infrastructure will be enhanced accordingly. And the live drills will continue.

Policy Support

BCP will have a different meaning for businesses that are not online. DR is simple for companies that do not have online systems. Most systems are manual, they have print-outs and even if their computers are down for three days, their business suffers minimal disruption.

Indian stock exchanges and brokering houses have been slow to move their transactions online. This has been mainly due to Government regulations. There was initial delay in laying down specifications for creating Closed User Groups (CUGs). The issue was resolved between the DoT and the Finance Ministry around 1998 and soon trade portals like ICICIDirect.com, motilaloswal.com, and smartjones.com came into being.

On March 21, 2000 an Ariane 5 was successfully launched from at Kourou, French Guiana carrying INSAT-3B, owned, built and operated by ISRO. It is primarily intended for business communication, developmental communication and mobile communication. The communication payload provides 12 extended C-band channels, each having a bandwidth of 36 MHz. The Ku-band payload provides three channels, having a bandwidth of 77/72 MHz. The Mobile Satellite Service transponders operate in C/S band frequencies.

The Department of Telecommunications now authorizes private satellite networks using VSAT antennas. Users (includes NSE) lease at least one quarter of a transponder for this purpose.

Along with the resolution of regulatory issues, India no longer has any pressing connectivity and bandwidth issues. With, the entry of private players into the broadband scenario and the government opening up the telecom sector, these issues are almost non-existent. Security solutions and services available in the market have matured and it doesn't cost heavily to put a simple backup solution in place.

Change Management Strategy

Approach

Challenges encountered while setting up a BCP/DR site

Broadly, there are two types of challenges—technical and non-technical (people/management). The first and the biggest challenge was convincing top management that business continuity (BC) investment is essential.

Companies could suffer huge losses in business each day due to downtime. NSE's daily turnover (total worth of all transactions each day) is Rs 2,000 - 3,000 crore. The resulting damage could be both tangible and intangible.

- Tangible: Loss of assets.
- Intangible: Loss of business, loss of credibility/image.

The second challenge was deciding how much to replicate and how much time was needed for the switchover.

The third challenge was to give realistic requirements (for decisions like switchover time definition).

The fourth challenge was to involve *all groups in business continuity planning* (BCP). Complete BCP cannot be achieved unless all user groups are involved, including top management.

The fifth challenge was handling change and maintaining the BC policy. A BCP may hold well in the beginning. But as time goes by, infrastructure is upgraded, new applications are installed, and changes are made in existing applications and configurations — so the plan may not be comprehensive after six months. The challenge is to keep the backup site synchronous with the primary site—at all times.

The sixth challenge was to conduct regular drills and test the BCP, and keep it up to date. Such drills are carried out once a month.

Deployment Model

Strategy for deployment

The reasons for choosing Chennai as the new DR site venue are:

- Mumbai and Pune are in the same seismic zone.
- Chennai is in a relatively less sensitive seismic zone.
- Data has to be replicated daily at the DR site. But Pune at that time did not have very good connectivity options from telecom and ISPs.
- NSE wanted the DR site in a state with a different political climate.
- The staff at Pune was underutilized. Personnel at the well-staffed DR site in Chennai are also involved in development and management of applications when there are no disasters and drills.

What to replicate at the DR site?

NSE used three policies to govern what to replicate at the DR site:

First - All business critical applications must run without compromise. *Applications like trading, clearing and settlement; surveillance, position monitoring, and risk management are mission critical and require guaranteed response.*

Second - Certain other applications operations will continue to run, but may show less response time and performance levels.

Third - In case of disaster, certain applications will not be performed at all. *Delivery deadlines for these applications, like software development and benchmark testing, may be extended.*

This is mainly because the primary site has adequate resources. But the DR site may not have those luxuries. A process of resource optimization is necessary at the DR site.

Business Continuity Plan (BCP) of NSE provides for replication of *entire technology infrastructure at a remote site.*

The site was a mirror of the entire infrastructure including the satellite earth station and a high-speed optical fibre link of NSE's Mumbai office. The transaction data is backed up on a real-time basis from the main site to the disaster recovery site through a 2 Mbps high-speed link, which keeps both the sites synchronized with each other. Additionally, the day's entire transaction data is backed up on the portable magnetic storage media. Of this two copies are created: One is stored in a fireproof cabinet located at the main site and the other, in a separate cabinet located on a different premises. The entire DR site infrastructure at Pune was moved to Chennai.

Applications for DR

8 **Stratus Fault-tolerant Mainframe Class machines** run the critical applications at the primary site. They also run other non-mission critical applications like development, testing, load testing, benchmarking, and simulation. The DR site has three such machines that only replicate the critical applications. *The non-mission critical applications are not run during a disaster.*

A number of **Unix servers** and the **Oracle database** are used for back office activities at the primary site. These are typically clearing and settlement applications. NSE calculated the minimum critical mass needed to carry out these applications to be six servers. So the DR site has six Unix servers, which perform these applications. NT servers are used for mail applications.

The extranet server is hosted at the primary site and mirrored at an external ISP. This is because brokers can always connect to the external ISP through alternate routes via the Internet in case of a disaster.

Business Model

Description

Providing BCP and DR sites has considerable financial implications. Unless risk and cost-benefit analyses are carried out, it may be difficult to justify the investment to be made. *The average daily turnover in the capital markets segment at NSE is around Rs 2300 crore, with an average traffic volume of one million trades per day. In the derivatives segment, average daily turnover is Rs 1300 crore with a volume of around 50,000 trades per day. There are around 13,000 registered users in both segments and an average of around 9500 users is logged in at a time.* In an e-business marketplace it is essential for companies to assess the risks and quantify their financial and intangible impact on the business.

Factors critical to sustainability

While a separate DR site is a possibility for companies that have multiple sites, the huge costs for setting up a new site purely for DR does not make sense. The DR site remains on standby until a major disaster actually happens, and then, one questions the probability and frequency of natural disasters. Smaller companies may not afford hot sites and instead could use the datacenter for backing up data.

Avoiding overspending on DR

Ask the three questions based on business requirements.

1. **Which few applications are truly critical and require recovery within 24 hours to keep the business afloat?**
2. **Which applications require recovery in 48 to 72 hours? (May need only inexpensive tape backup)**
3. **Which applications require recovery after 72 hours? (May need nothing!)**

NSE is a for-profit exchange unlike most others, which are set up either as 'not-for-profit' companies or as associations of their respective members. The key revenue strategy adopted is that a stock exchange should generate most of its revenues through transaction execution and not through listing fees. NSE has been making profits and paying dividends from the first full year of its operations. It was set up with a share capital of Rs.100 million. Its net worth stood at Rs.2184 million on 31.3.2001.

Leadership

Key factors which led to success/failure

Information and Communication Technology is the key factor responsible for the success of NSE operations. The time taken to complete transactions has shrunk dramatically in favour of investors. Institutional ownership has enabled the NSE to adopt a business model that accords primacy to the interests of investors, with brokers just being service providers. The latter do not own and control the exchange – a position they have even today on the other exchanges, and have often abused over the decades.

Costs have shrunk for retail as well as institutional investors even as transparency has improved.

Impediments, if any

Connectivity is perhaps the most important technological factor. The cost of leased lines and VSAT links has been traditionally very high and the reliability of the links has been low. It also took a long time to commission the links, as one had to make an application and wait for a few weeks for the link to be up and running. Other issues like security, and backup and recovery procedural costs are also deterrents.

High infrastructure costs and expensive bandwidth, which are both prerequisites to have an efficient and effective DR, are one of the primary reasons behind the slow adoption of DR in India. But it is expected that in the coming years bandwidth rates and infrastructure costs will come down in India which will give a further boost to the domestic DR market.

One of the biggest challenges NSE faced was setting up a complete satellite earth station, at a suitable back-up site. And to do this, it was not so much of a technical challenge, but more a regulatory hurdle that NSE faced. For instance,

the company had to get various no-objection certificates from different authorities for setting up the site. The most crucial approval from SACFA (Standing Advisory Committee on Frequency Allocations) required for setting up the earth station took almost a year to get clearance. And finally Pune was decided as the ideal back-up site.

NSL has successfully overcome these impediments by application of technology and constancy of purpose of providing high quality service to customers.

Standard Operation Procedures

Norms for switching over to the DR site in an emergency

- For hardware, software or environmental problems, the staff determine whether the systems or applications are repairable and recoverable, and within what timeframe. In such emergencies, the engineers do spot assessment and troubleshooting. The first choice is to recover the same system as soon as possible.
- If the staff are not able to get back online (within a certain time), they switch over to a backup system within the same premises (at the primary site itself).
- But if even this is not possible—for instance there may be a major fire at the primary site—then the staff will take a decision to switch over to the backup site if they are not going to recover in a certain timeframe, say a few hours.
- Switching over to the DR site is the last resort, since the switchover takes time, and involves a set of operational procedures.
- But the switch cannot be instantaneous. The reason is that the transactions are conducted in real-time, and are held in memory. One transaction may be worth several crore rupees — and it could have a cascading effect (on other transactions). So switchover will be done with a fresh cycle, and copy previous transactions to the backup site.
- The switchover procedures are specific to each department/workgroup—and everything is well documented.
- The decision is taken on the basis of each situation.

A dedicated core team comprising both business and IT staff, is responsible for the entire BCP operations. The function of this group is to

- Ensure successful drills
- Update the checklist for BCP operations on a continuous basis
- Maintain exhaustive documentation on the BCP procedures, which includes details of classification of events falling under disaster category, and the corresponding action plan.

In the event of an actual disaster, a nominated commander of the BCP team would assume charge and control operations from a pre-allotted command room.

Back up of transactions

NSL has two ways of backing up.

a. Backup for the backend transactions (like clearing and settlement) are done on an event or online basis. The time taken to backup depends on the transmission time for data transfer.
b. There is the trading data, which is inside memory. This data is transferred to the backup site at the end of the day.

Cost

NSL has invested close to Rs 40 crore in building up its backup site. But it is not complaining, as research has shown that most companies without a proper disaster plan have been totally wiped out.

Artifacts

The following sites provide information on Disaster Recovery that includes papers, videos and software.

- http://www.rothstein.com/data/cg090001.htm
- http://www.rothstein.com/data/cg040001.htm
- http://www.rothstein.com/data/cg050001.htm
- http://www.rothstein.com/data/cg060001.htm
- http://www.rothstein.com/data/cg070001.htm
- http://www.rothstein.com/articles.html

Glossary of Stock Exchange Terms used

Capital - Capital is an extremely vague term that depends on the context for a specific definition. In general, it refers to financial resources available for use.

Clearing - The procedure by which an organization acts as an intermediary and assumes the role of a buyer and seller for transactions in order to reconcile orders between transacting parties.

Debt - An amount of money owed from one person or firm to another. Bonds, loans, and commercial paper are all examples of debt.

Derivative - A security, such as an option or futures contract, whose value depends on the performance of an underlying security. Futures contracts, forward contracts, and options are the most common types of derivatives. Derivatives are generally used by institutional investors to increase overall portfolio return or to hedge portfolio risk.

Equity - A term describing stock, or any security, representing an ownership interest. Equity is a term whose meaning depends very much on the context. In general, you can think of equity as ownership. For example, stocks are equity because they represent ownership of a company, whereas bonds are classified as debt because they represent an obligation to pay and not ownership of assets.

Exchange - Exchange is a market in which securities, commodities, options, or futures are traded.

Futures - A financial contract that encompasses the sale of financial instruments or physical commodities for future delivery, usually on a commodity exchange. Futures contracts try to "bet" what the value of an index or commodity will be at some date in the future.

Mutual funds and large institutions to hedge their positions when the markets are rocky often use futures.

IPO (Initial Public Offer) - The first sale of stock by a private company to the public is known as IPO. IPOs are often smaller, younger companies seeking capital to expand their business.

Mutual Fund - A security that gives small investors access to a well-diversified portfolio of equities, bonds, and other securities. Each shareholder participates in the gain or loss of the fund. Shares are issued and can be redeemed as needed. The fund's net asset value (NAV) is determined each day. Each mutual fund portfolio is invested to match the objective stated in the prospectus.

Online trading - Making trades via the Internet.

Option - A privilege sold by one party to another that offers the buyer the right, but not the obligation, to buy (call) or sell (put) a security at an agreed-upon price during a certain period of time or on a specific date.

Risk - The chance that an investment's actual return will be different than expected. This includes the possibility of losing some or all of the original investment. It is usually measured using the historical returns or average returns for a specific investment.

Security - An instrument representing ownership (stocks), a debt agreement (bonds), or the rights to ownership (derivatives). A security is essentially a contract that can be assigned a value and traded.

Examples of a security include a note, stock, preferred share, bond, debenture, option, future, swap, right, warrant, or virtually any other financial asset.

Share - Certificate representing ownership in a company.

Stock - Stock is a type of security that signifies ownership in a corporation and represents a claim on part of the corporation's assets and earnings.

There are two main types of stock: common and preferred. Common stock usually entitles the owner the right to vote at shareholder meetings and to receive dividends that the company has declared. Preferred stock generally does not have voting rights, but has a higher claim on assets and earnings than the common shares. For example, owners of preferred stock receive dividends before common shareholders and have priority in the event a company goes bankrupt and is liquidated.

Also known as shares, or equity.

Trading - Trading is a transaction involving the sale and purchase of a security.

VaR - A technique used to estimate the probability of portfolio losses based on the statistical analysis of historical price trends and volatilities. Banks, security firms, and companies that are involved in trading energy and other commodities commonly use VaR. VaR is able to measure risk while it happens and is an important consideration when firms make trading or hedging decisions.

Annex 1

Operational Best Practices for DR & BCP

1. *Establishing a service-level agreement.*
   All disaster recovery and business continuity work begins with an agreement on what matters most to the business. For example, if access to a trading-floor application is lost for 15 minutes, the financial effect can be tremendous. This agreement forms the basis for service-level agreements (SLA) about IT performa nce.

2. *Identifying potential problems with achieving the SLA.*
   Developing scenarios that outline exactly what could go wrong and what it would take to mitigate it, ranking these scenarios for probability and cost and prioritizing them for executive approval. Agreement on projected losses gives a realistic idea of the resources required for continuity.

3. *Performing data classification.*
   Data classification reflects data availability requirements and in turn determines storage infrastructure for business continuity. Overlooking this step may lead to overspending on BCP.
4. *Deciding the risk thresholds for different areas of the business.*
   This enables making intelligent decisions. For instance, a server has failed. If the recovery time objective is 30 minutes and it takes 15 minutes to identify a problem, the recovery time may exceed 30 minutes.
5. *Develop detailed procedures for each scenario approved.*
   The failure scenarios selected are the basis for disaster recovery and business continuity planning and need to be adequately communicated to all architects and developers to ensure consistency in approaches to application development and infrastructures. Failure scenarios shine a light on the risks so that all are engaged in mitigation.
6. *Test*
   Testing may reveal new options or the elimination of certain failure scenarios that should be factored into the final release.

Seven Items Often Overlooked in Disaster Planning

-Dr.Steven Lewis

1. Missing things "too close to see"
2. Ignoring employee's relevant personal-life situations
3. Failure to track out-of-the-ordinary situations
4. Intuitively assuming how other departments function
5. Not learning needs of emergency organizations outside of the company
6. Forgetting "unforgettable" events
7. Ignoring external factors

http://www.rothstein.com/articles/seven.html

Annex 2

A practical case of disaster recovery

A case of Disaster Recovery - News Story by John E. Columbus, Columbus Consulting Group

Year of Disaster: July 1987
Company: *Bond House in Bloomington, Minnesota (more than 300 employees)*
Computer Systems: *Wang 2200*
Cause of Disaster: *Massive Rainstorm and Parking Ramp & Open Parking Area Sloping towards the Building, Back up of Sewer Water*
Effects of Disaster: *Flooding of parking area and building basement including form storage, media storage, power and phones. All computer systems were fine on the 22nd floor, but no electricity or forms for them.*

DRP: *The disaster occurred on a Friday night leaving Saturday and Sunday for planning. The plan examined the following possibilities.*

a. *Putting a generator on the roof to operate ventilation and power PCs.*
b. *Locating a warm site where Wang 2200s, terminals and a few PCs could be brought and setting up a phone connection to the company's California office to do data entry.*
c. *Transferring Bond House phone numbers to its branch office in St. Paul that was still functional and setting up accounting functions there.*
d. *Determining if the Forms Company had our forms or if they could quickly make more.*
e. *Having all employees meet at Bloomington site to discuss the situation.*
f. *Explaining that securities cannot be sold until the computers were operational, as per Securities and Exchange Commission rules.*

DRP implementation:

a. *A commercial real estate agent who had open office space with a small computer room was closeby.*
b. *A former phone technician who was on company's payroll was located and he was able to reroute a phone line from another tenant of the building to use with our California office.*
c. *The forms supplier did have some forms that could tide over until more could be created.*
d. *The local fire marshal and building inspector nixed the plans to either fly a generator to the roof or snake cables up the side of the building for 22 floors.*
e. *The building wouldn't be usable for another two weeks, and the computers wouldn't be returned from the warm site to the Bond House building until one month after the disaster.*
f. *There were no spare Wang 2200s immediately available. The existing machines (20- to 100-lb. down 22 floors-44 flights of stairs) amid high heat and humidity had to be hand-carried and then transported to our warm site.*
g. *The local Wang Support Company could rebuild the drives that didn't survive being bumped going down the stairs and we could reload them from the last backup that didn't get to the now submerged vault. Though the vault remained relatively dry, there was no way to reach it until the water receded.*
h. *Once everything was rebuilt and back online, data was updated and started selling securities again.*
i. *Working positions were re-established by Thursday and start selling securities.*

Lessons learnt:

a. Business interruption insurance is mandatory.
b. Disaster Recovery Plan takes time and it should have multiple options. (For example, in this case, a real estate agent was located, but the fire marshal and the building inspector rejected the generator plan.)
c. Employees should work in shifts to avoid burning out.
d. Building company relations with local establishments will be helpful.
e. Mobile phones are a must for communication during disasters.
f. Spare forms must be kept in another location.
g. Leasing equipment and services from other companies works in a disaster.
h. The assets the company still has functioning should be used to greater capacity if possible while the disaster site is brought online. Phones are especially important because customers are worried about what's going on.
i. Restoring sales is the No. 1 priority, because cash flow is needed for survival.
j. Disasters are very expensive and usually happen without notice. Good public relations are critical to avoid losing market share.

The Case - Disaster Recovery Plan of the National Stock Exchange Limited, Mumbai.

Policy

- DoT and the Finance Ministry have resolved the issue of laying down specifications for creating Closed User Groups in 1998 allowing private trade portals for online transactions.
- The Department of Telecommunications now authorizes private satellite networks using VSAT antennas. Users (includes NSE) lease at least one quarter of a transponder for this purpose.
- Along with the resolution of regulatory issues, India no longer has any pressing connectivity and bandwidth issues. With, the entry of private players into the broadband scenario With the GOI opening up the telecom sector, the connectivity and bandwidth issues are almost non-existent.
- Security solutions and services available in the market have matured and it doesn't cost heavily to put a simple backup solution in place.

The context

Till recently, ICT-intensive companies were paying lip service to the idea of a BCP/DR. Increased threat of attacks like power outages, fires, floods and terrorism (9/11 WTC Disaster) coupled with regulations stipulated by regulatory bodies to ICT-dependent businesses and international competition have all made these businesses to seriously plan and implement/maintain BCP/DR.

NSE needed to set up a Disaster Recovery (DR) infrastructure to:

- Attract international investors
- Offer Business Continuity (BC) during a disaster

- Follow BC policies

The project

The National Stock Exchange of India Limited is a pioneer in planning and maintaining a secondary DR site at Chennai so that its operations can continue in the event a disaster strikes.

- Ensures uninterrupted service by NSE through adequate measures to support business recovery, which includes a DR site in another city.
- The goal is primarily BCM. In the case of the severest damages, NSE should be up and running within the shortest possible time.
- The DR plans are continuously updated and in the event of a disaster, NSE can be back in business within 24 hours.
- NSE set up its first DR site in Pune. The DR site was migrated to Chennai in 2002. This has made NSE the only exchange in India with a live DR site.
- Systems have been designed to switch over in such a way that NSE would be online again the very next day. But if a disaster occurs at the beginning of the day (before the market opens), NSE could be online in an hour's time (by switching to the backup systems at the primary site itself).

Challenges

- Convincing top management that business continuity (BC) investment is essential to minimize tangible and intangible business losses.
- Deciding how much to replicate and how much time was needed for the switchover.
- Giving realistic requirements (for decisions like switchover time definition).
- Involving all groups in business continuity planning (BCP).
- Handling change and maintaining the BC policy to keep the backup site synchronous with the primary site—at all times.
- Conducting regular drills and testing the BCP, and keeping it up to date.

The success factors

- Information and Communication Technology is the key factor responsible for the success of NSE operations.
- Identification of a minimum number of critical business processes and resources to maintain an acceptable level of business in the event of a disaster by carrying out *business impact analysis*.
- Ensuring that the requirements of online and real-time data could be restored as quickly as possible.

Lessons

- The *biggest risk to business continuity* is the lack of conviction among the top executives of the enterprise that a risk actually exists. Enterprises have to be proactive in formulating and maintaining Business Continuity Management Plan more seriously and not wait for disaster to strike first.
- Senior management can be convinced by presenting alternative strategies for disaster recovery (including alternative storage sites), the risk associated with each strategy, and cost benefit analysis of recovery strategies and not by pressurizing psychologically or demands of regulatory requirements.

FINAL REPORT

APPENDIX 14

14. NSE Supplier and Impact Questionnaire and Response

Your Name:	OSITA OGBONNAYA	**Title:**	DEPUTY GENERAL MANAGER – INFORMATION TECHNOLOGY & MARKET OPERATIONS
Job Function	INFORMATION TECHNOLOGY & OPERATIONS	**Reports to:**	GENERAL MANAGER – INFORMATION TECHNOLOGY & MARKET OPERATIONS
Date:	May 13, 2010		

Background

This Questionnaire Guide is used to gather your input into the final preparation of the NSE Disaster Recovery Planning & Business Continuity Planning project.

Once we receive your input, GIT will complete Tasks 10 and 11 (the Final Task). To accomplish this, GIT will prepare and conduct a meeting to present, review and summarize the information developed in completing the earlier Tasks. GIT will prepare and deliver to the NSE and USTDA a comprehensive final report of all work performed under the Terms of Reference ("Final Report").
The Final Report includes all deliverables and documents that have been provided to the NSE. The Final Report will be prepared in accordance with Clause I of Annex IT of the Grant Agreement. The Final Report includes an Executive Summary and all deliverables. Each task of the Terms of Reference forms a separate chapter of the Final Report. The Final Report includes a list of suppliers, including potential sources of U.S. equipment and services, relevant to the implementation of each component of the Project.
The Final Report is prepared in English. GIT shall provide five (5) hard copies and one (1) electronic version of both the confidential and public versions of the Final Report to the NSE and provide copies to USTDA in accordance with Clause I of Annex IT of the Grant Agreement.

NSE BCP/DRP Project

FINAL REPORT

THE Nigerian STOCK EXCHANGE

GENERAL INSTRUCTIONS

GIT is responsible for compliance with U.S. export licensing requirements, if applicable, in performance of the Terms of Reference. GIT and NSE must be careful to ensure that the public version of the Final Report contains no security or confidential information. **ENTER** the information that "best" represents your specific understanding about local Suppliers, Development and Environmental Impact for NSE. Identify any items that you believe are confidential and should NOT be in the "public" version of the report.
Please enter as much clarifying information as you can.
Note: All of the information entered this questionnaire will be held in strict confidence.

PLEASE RETURN THE COMPLETED GUIDE FILE WITHIN ONE WEEK AFTER YOU RECEIVE IT
Next Steps:

1. **Complete the Questionnaire and return a readable "soft"-copy**
2. **The GIT project team will consolidate Results**
3. **The GIT project team will prepare the final DRP and present to NSE**
4. **The GIT project team will continue to work with you.**

If you have any questions, please call or contact: Mike Ike, Irv Brownstein or Dan Nebel

Thank You!!

INFORMATION TYPE	NSE RESPONE DATA	EXPLANATION
TASK 7: SUPPLIER IDENTIFICATION		
Can you identify potential suppliers of computer software, hardware and support in Lagos? Note: This information is needed in sufficient detail that the NSE can make informed, responsible decisions regarding product or service procurement. GIT will also identify U.S. sources of supply for the equipment in accordance with the USTDA Agreement (Clause I of Annex II)	Software vendors: • PROGENICS Corp Limited • Global InfoSwift Technologies Limited • Allied Soft Nigeria Limited • Info Soft Nigeria Limited • Dimension Data • Telnet Nigeria Limited Hardware/equipment vendors: • Dimension Data • Global InfoSwift Technologies Limited • Net Solutions Limited • CIS Nigeria Limited • Computer Warehouse Limited • KECAM Ventures Nigeria Limited • Telnet Nigeria Limited Other key vendors: • Right Click Nigeria Limited • New Dawn Technologies Limited • Brent Technologies Limited	By Type: • A minimum two vendors each. • Name, Address • Focus of offering

INFORMATION TYPE	NSE RESPONE DATA	EXPLANATION
TASK 8: DEVELOPMENT IMPACT ANALYSIS		
Can you identify any potential <u>development impacts</u> for the project in Nigeria?	<u>Any Potential Development Impact(s):</u> • Once The NSE successfully operates a true disaster recovery and business continuity management culture, we will have systems that are more effective; more efficient; more nationally and internationally utilized than our competitors. At such point, we will be able to maximize the return on investment (for The NSE and her partners) we made in business processes. We will be more productive, more reliable and an excellent partner and service provider. When we set deadlines, we will meet it. When we undertake a project, we will deliver on time and on budget. In this way, business continuity management becomes necessary not because it means we will survive into the distant future; but because it will make us a better and more competitive business today for all our stakeholders. • Analyze the impact of a business disruption and the cost of downtime, then assess and address any gaps. • Manage risk through an enterprise-wide resiliency strategy • Reduce cost through proactive incident response and reduced downtime • Ensure resilient service delivery in a 24-hour, 7-day-a-week world • Respond with speed and agility while minimizing risk exposure •	**Yes – describe – or No**

INFORMATION TYPE	NSE RESPONE DATA	EXPLANATION
Can you identify any additional developmental benefits of the Project for the Exchange?	Security Benefits • Ensure your data is effectively backed up and easily recovered. • Protect valuable information assets: Prevent loss of business information from site disasters, viruses, human error, and application and system failures by providing alternate remote and local copies of data and enabling rapid restart and recovery. • Consolidation is perhaps the most obvious and popular means of enhancing IT service levels while simultaneously improving controls as well as lowering costs. Reliability Benefits • Assess how you can reinforce your business processes so that when unexpected disruptive events occur, NSE customers and NSE partners remain in contact and your brand stays strong • Enable NSE workforce to continue working in times of disruption. • Protect the NSE brand through industry-leading disaster response and recovery platform and processes • Having a top-quality, tried and tested disaster recovery and business continuity management structure in place will help The NSE stand out from others. Data Integrity Benefits • Deployment of a solid DR/BC management structure and infrastructure guarantees availability of data that is less prone to corruption, manipulation and loss. Other Benefits	**Yes – describe – or No**

INFORMATION TYPE	NSE RESPONE DATA	EXPLANATION
	• Determine the constantly changing governmental and industry regulations associated with business continuity that apply to you and help develop a plan for compliance. • Standardize IT practices on fewer storage platforms: Gain improved performance and greater scalability and availability; reduce burdens on IT staff • It can help to create a business that operates its systems to the optimum level. Business continuity management involves creating resilient businesses; companies that are flexible and which can quickly identify and respond to challenges and threats. However, resiliency is not just a benefit in times of disaster. Resiliency can provide day-to-day business benefits with hardened systems failing less often and production returning more quickly from day-to-day glitches than would be the case in less resilient businesses. In other words, business continuity management is about optimizing process availability; and this enables businesses to operate to maximum efficiency at all times.	
Can you Estimate the Project's potential benefits in each of the following areas?	**Infrastructure / Industry** • Veritable platform for the capital market • Further strengthen positive perception of the market • Increase in investor confidence in the market • Enthrones best practice for other arms of the market to follow • Drive growth in the industry • Positions the market to attract more FDIs • Prepares the Stock Exchange to join the league of global players • The business that recovers most quickly from a wide-area disaster is the	**Yes – describe – or No**

INFORMATION TYPE	NSE RESPONE DATA	EXPLANATION
	business which is able to capitalize on the situation. Disasters create new markets and open up existing ones. This may allow the rapid development and launch of new products	
	Market-Oriented Reforms • This will further support current reforms and transformation programs already embarked by both The Stock Exchange and SEC • It will fall in line with recommendations made for market improvement in the areas of enhanced information availability and integrity of data. • It will guarantee transparency and fairness in the market which will translate into investor confidence • It is well documented that an effective disaster response can help a company's share price to increase and its reputation to become stronger. Therefore the project will enhance perception of The NSE and positive impact on our overall rating as a market and organization	Any regulations, laws, or institutional changes recommended? What affect would they have if implemented? **Yes – describe – or No**
	Human Capacity Building • Three types of training will be conducted, namely: Technical, Operational and End User Trainings. • Technical Training will focus on the architecture, infrastructure and configuration of the various platforms to be deployed for the DR/BC. • Operational Training will focus on day to day procedures and management of the DR/BC procedures and maintenance of a continuous state of preparedness. • The End User Training will involve educating every one of their roles during a DR/BC operation and their roles in maintaining preparedness	Estimate the number and type of positions that would be needed to implement, manage, and operate the proposed Project. How many people will receive training? What kind of training program would be needed?

INFORMATION TYPE	NSE RESPONE DATA	EXPLANATION
	for any eventuality	**Yes – describe – or No**
	Technology Transfer and Productivity • Increased WAN capacity and WAN upgrades • Adequate training and mentoring must be put in place to ensure knowledge transfer and sustainability of all processes and procedures • Regular knowledge updates and technology upgrades must be part of the maintenance and support agreement with the vendors. • Productivity will result through reduction or elimination of downtime, access to data and information will be available to all stakeholders thereby increasing task completion and eliminating reworks and unnecessary errors, misrepresentation and correction • Use resources and personnel efficiently: Offload processing and data to alternate systems and locations; use advanced software tools to minimize the labor intensive nature of backup and recovery procedures	Any advanced technologies that will be implemented as a result of the Project? What type(s) of productivity and efficiency gains do you think will result? **Yes – describe – or No**
	Other. • Simplify disaster recovery: Achieve rapid restart/recovery over virtually any distance with minimal impact on application response time; eliminate inefficient and resource intensive tape-based replication or retrieval systems •	Any other developmental benefits of the Project, including any spin-off or demonstration effects? **Yes – describe – or No**

INFORMATION TYPE	NSE RESPONE DATA	EXPLANATION
TASK 9: PRELIMINARY ENVIRONMENT IMPACT ASSESSMENT		
Are there any potential environmental impact to local requirements and those of the World Bank?	• NO	**Yes – describe – or No**
How would you mitigate each impact if and when the Project moves to implementation?	• NO	**Yes – describe – or No**

APPENDIX 15

15. The Nigerian Stock Exchange Proposed Organization Plan & Charts

PROPOSED ORGANIZATION PLAN & CHARTS

APRIL, 2006

CONTENT

	Page
Highlights of this Proposal	2
Current Organization Plan	3
Proposed Organization Plan	4
Office of the Director General	5
Quotation/Listing Division	6
Listing & Monitoring Department	7
Emerging Markets Department	8
Operations Division	9
Information Technology & Market Control Department	10
Compliance Department	11
Branch Operations Section	12
Bonds/Derivatives Markets Division	13
Support Services Department	14
Human Resources / Admin. Section	15
Finance/Accounts Section	16
Corporate Affairs Section	17
Proposed NSE Comprehensive Organogram	18

Appedix Details begin on Next Page

THE NIGERIAN STOCK EXCHANGE

PROPOSED ORGANIZATION PLAN & CHARTS

APRIL, 2006

	Page
Highlights of this Proposal	2
Current Organization Plan	3
Proposed Organization Plan	4
Office of the Director General	5
Quotation/Listing Division	6
Listing & Monitoring Department	7
Emerging Markets Department	8
Operations Division	9
Information Technology & Market Control Department	10
Compliance Department	11
Branch Operations Section	12
Bonds/Derivatives Markets Division	13
Support Services Department	14
Human Resources / Admin. Section	15
Finance/Accounts Section	16
Corporate Affairs Section	17
Proposed NSE Comprehensive Organogram	18

HIGHLIGHTS OF THIS PROPOSAL

1 . Creates **three** main **Divisions** namely, the **Operations, Quotations/Listings** and the **Bonds/Derivatives Market** each to be headed by an **Executive Director.**

2 . The **Quotations/Listings Division** to comprise the following **Departments**.
(i) Listing & Monitoring
(ii) Emerging Markets

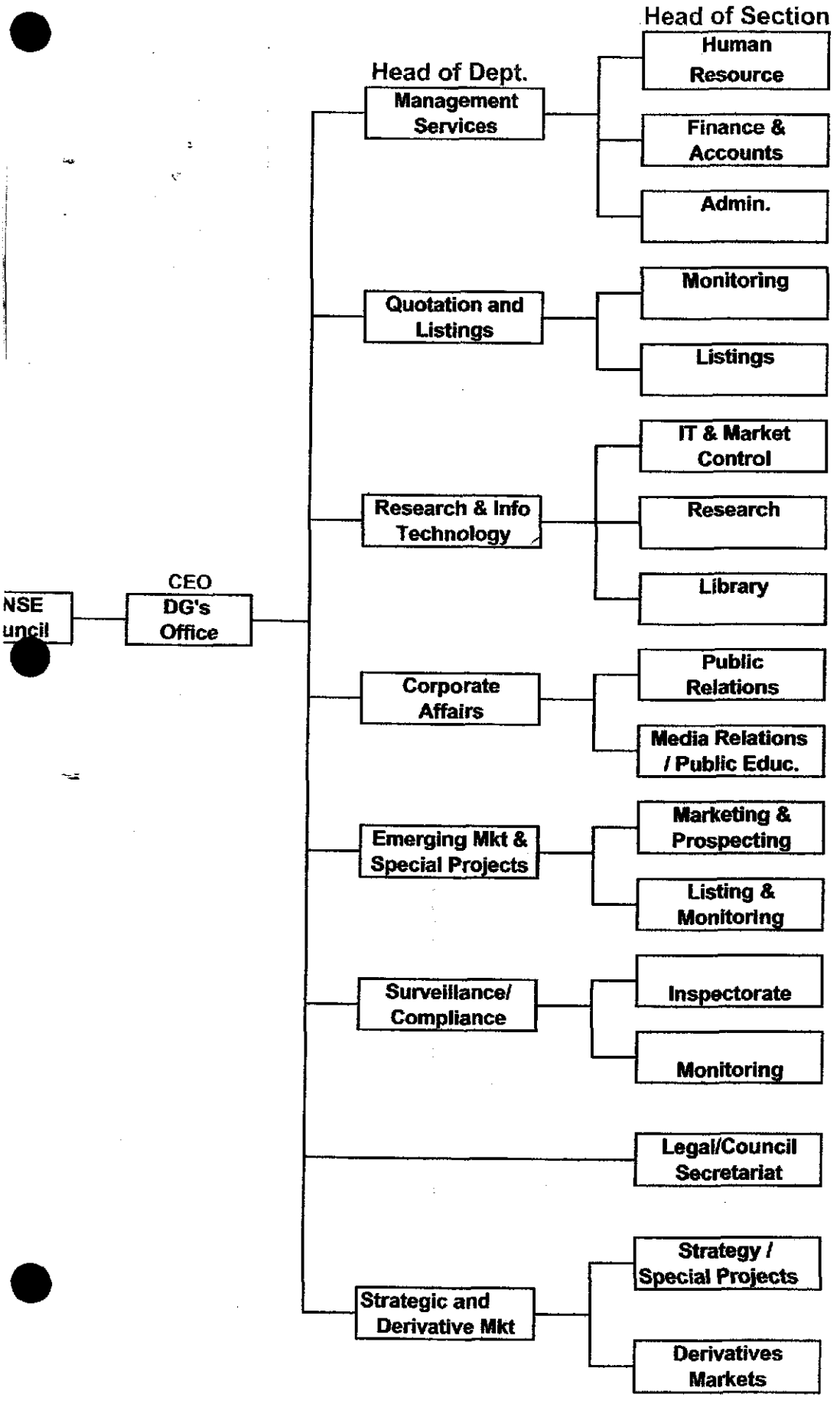
3 . Constitutes the following **Departments** into the **Operations Division**.
(i) Information Communications Technology & Market Control
(ii) Compliance
(iii) Branch Operations

4 . The **Bonds & Derivatives Markets Division** consists of the following **Departments**.
(i) Bonds & Derivatives Markets
(ii) Research & Library Services

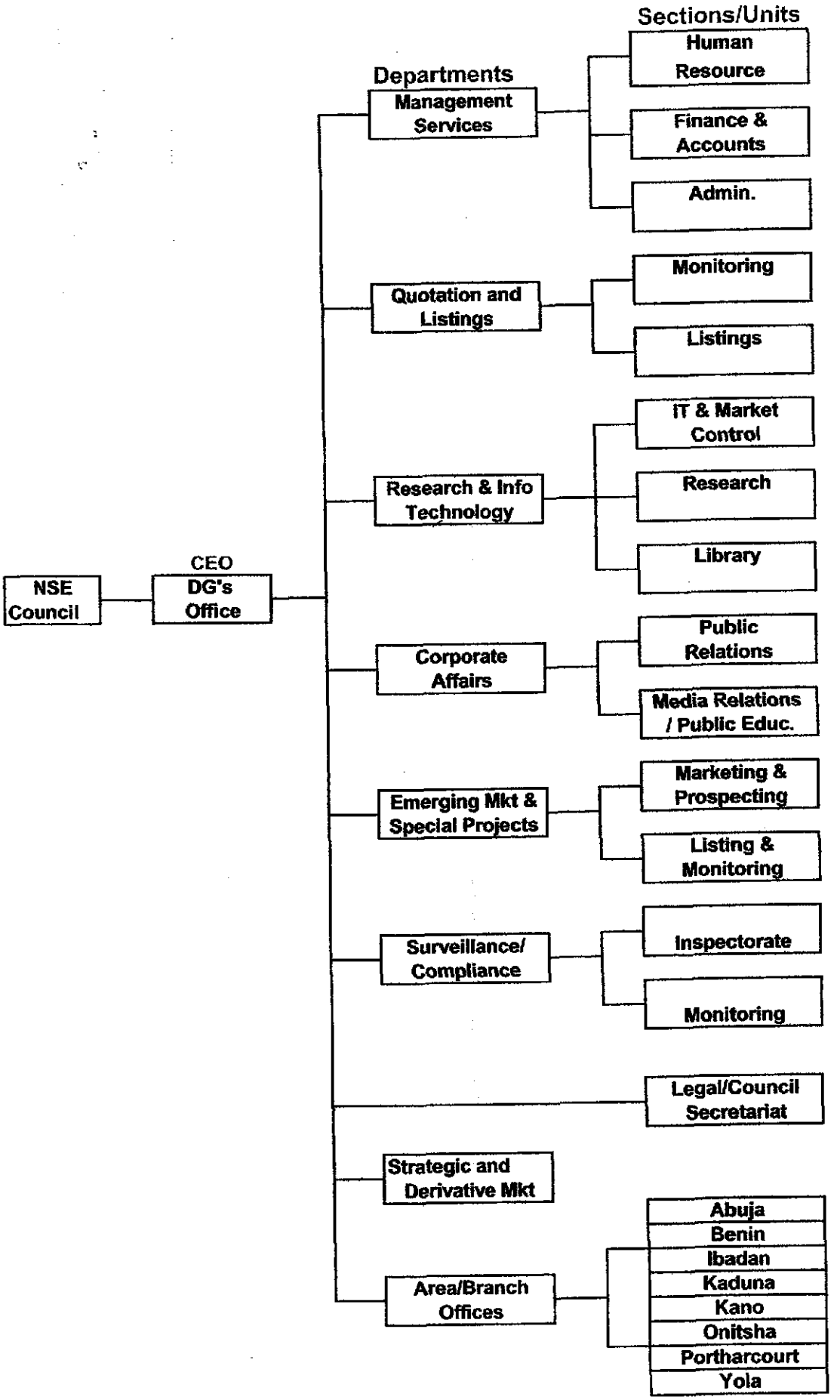
5 . The following **functions** shall be grouped under **Support Services Department** and will be **headed** by a **General Manager** attached to the **office of the Director General.**
(i) Human Resource & Administration
(ii) Finance/ Accounts
(iii) Corporate Affairs

6 . Creates the following **Units** which shall **report to the Director General.**
(i) Internal Control
(ii) Legal/Council Secretariat
(iii) Strategy

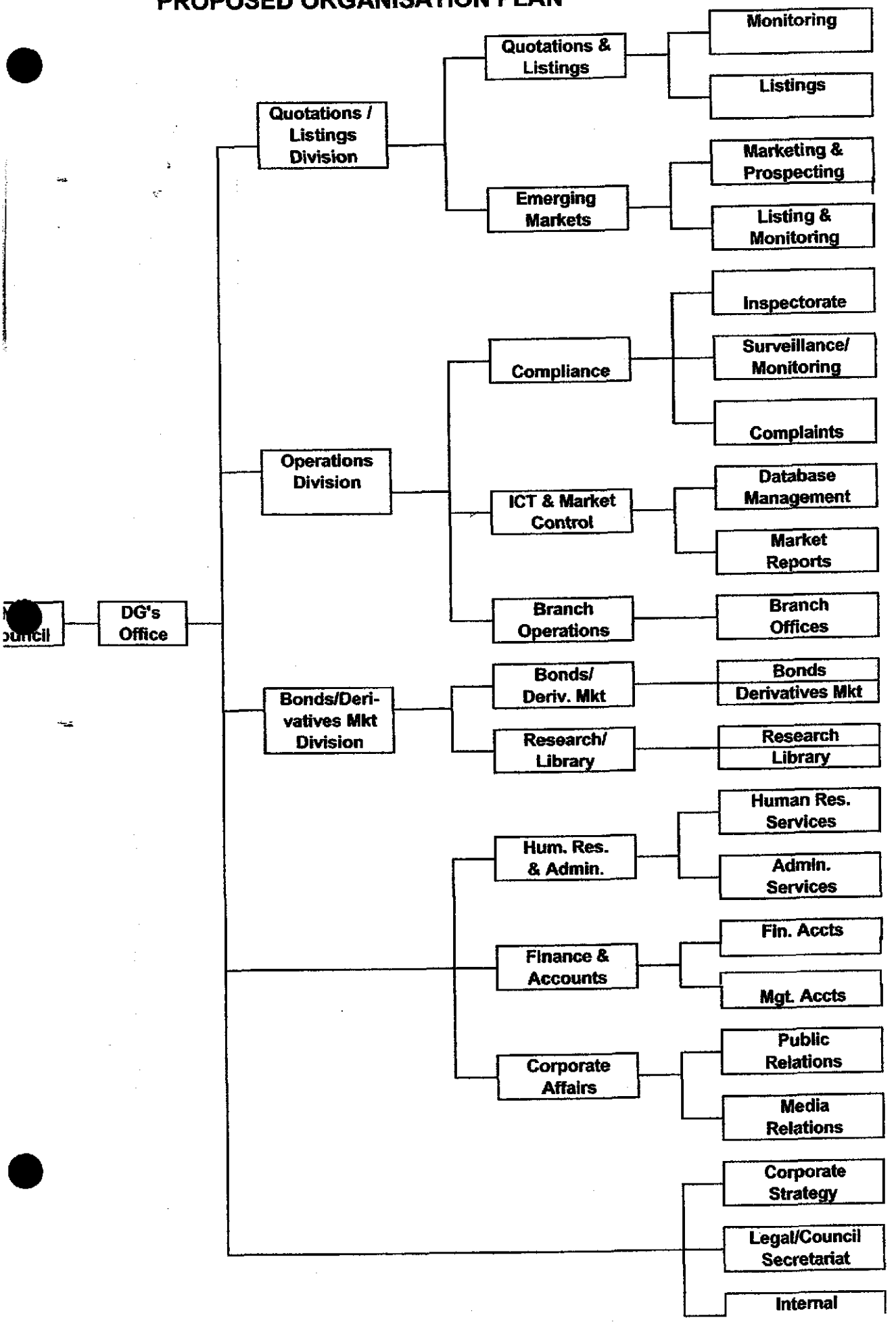
CURRENT ORGANISATION PLAN: HEAD OFFICE



THE NIGERIAN STOCK EXCHANGE
CURRENT ORGANISATION PLAN: HEAD OFFICE

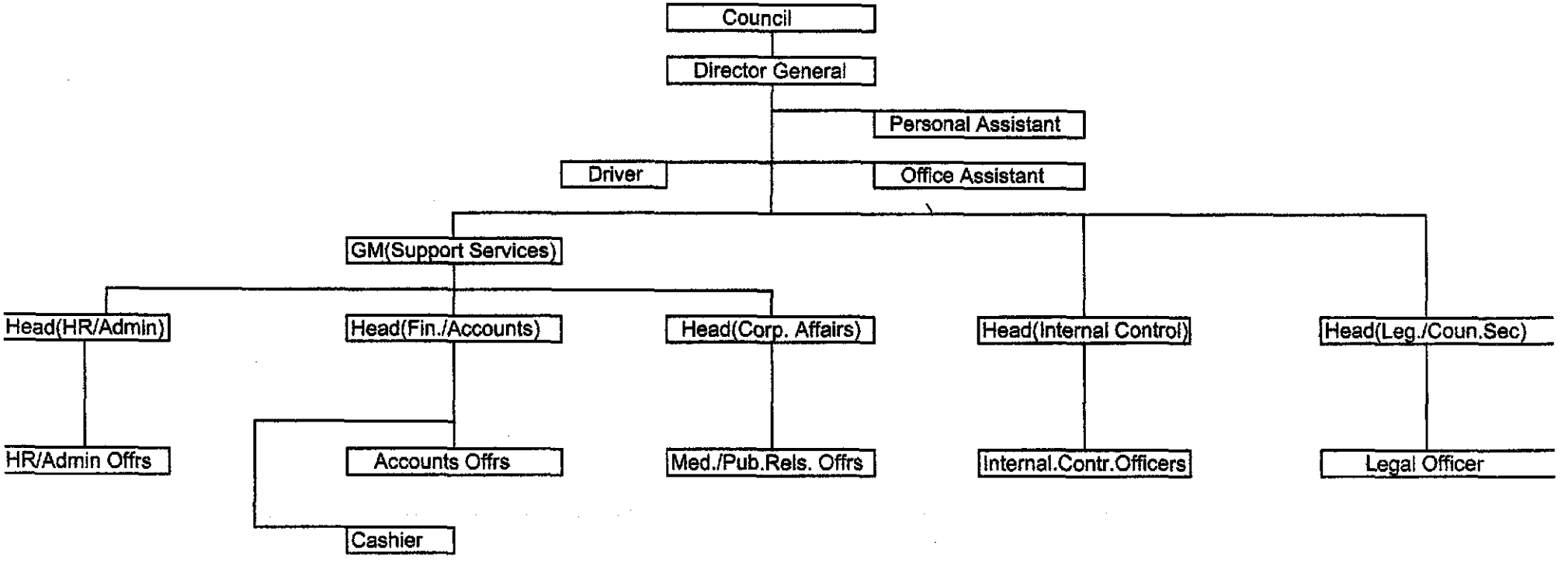


PROPOSED ORGANISATION PLAN



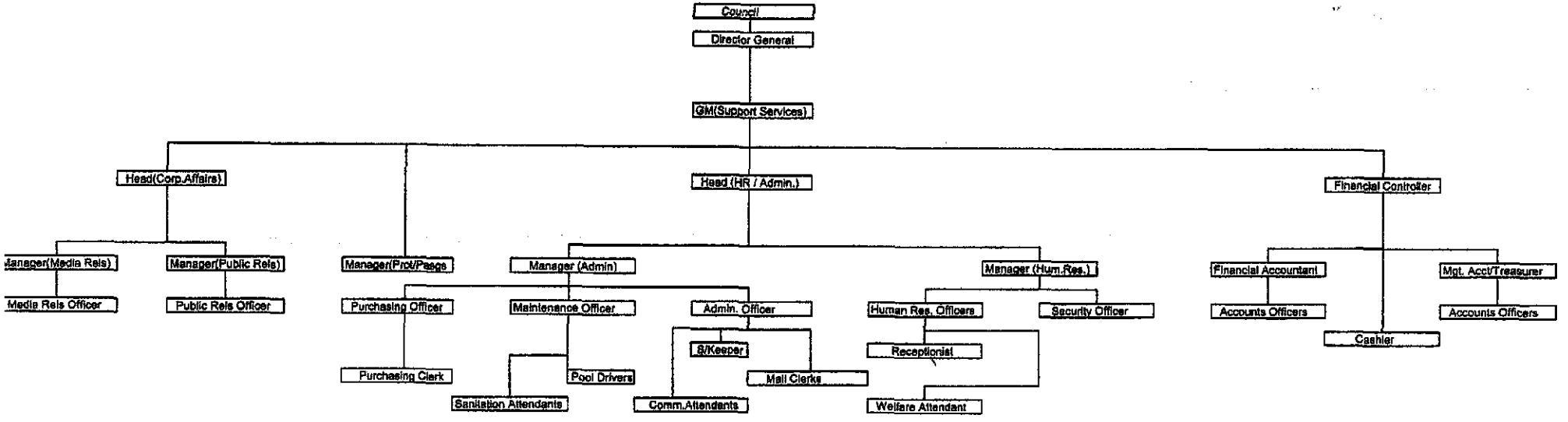
THE NIGERIAN STOCK EXCHANGE

OFFICE OF THE DIRECTOR GENERAL
PROPOSED ORGANIZATION CHART



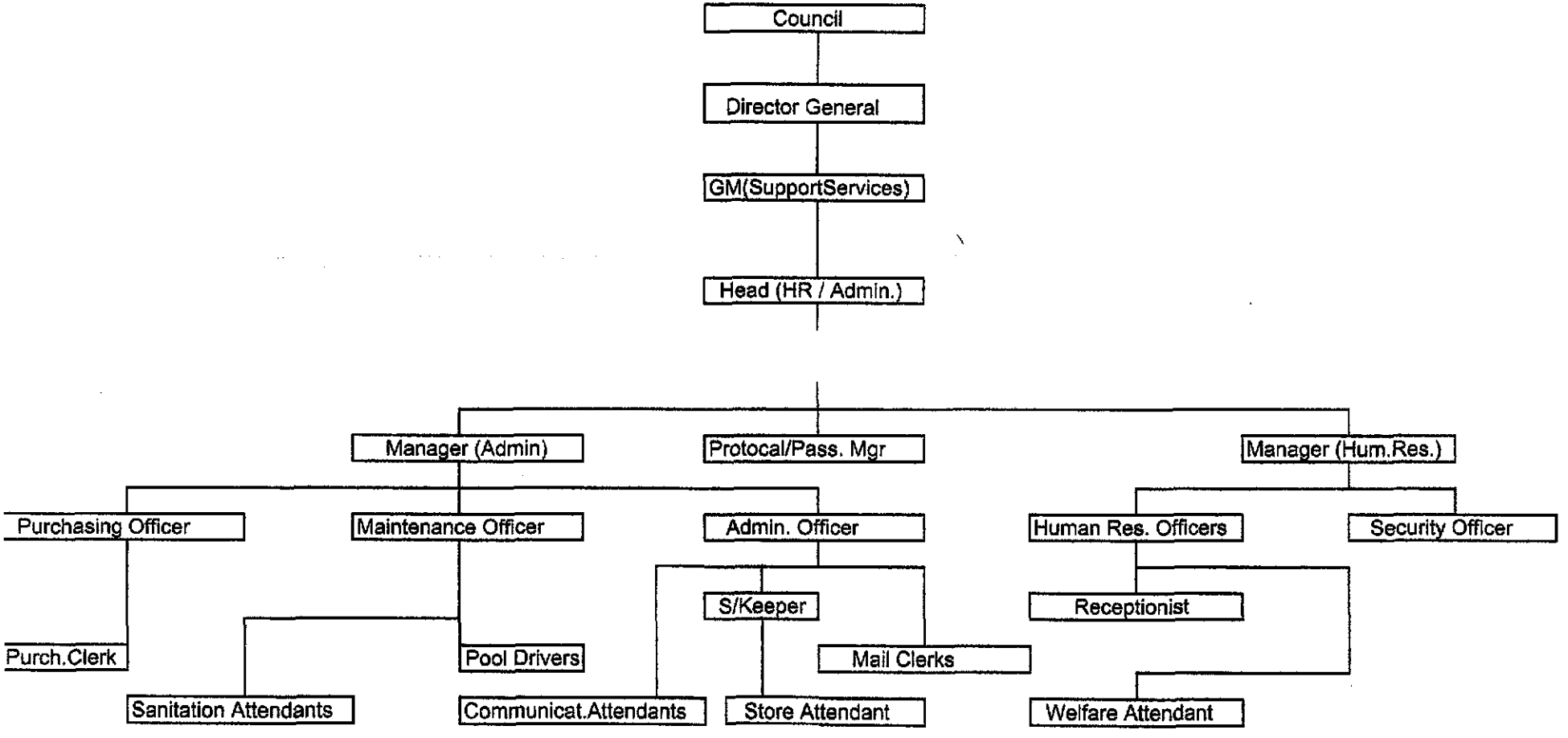
THE NIGERIAN STOCK EXCHANGE

SUPPORT SERVICES DEPARTMENT
OFFICE OF THE DIRECTOR GENERAL
PROPOSED ORGANIZATION CHART



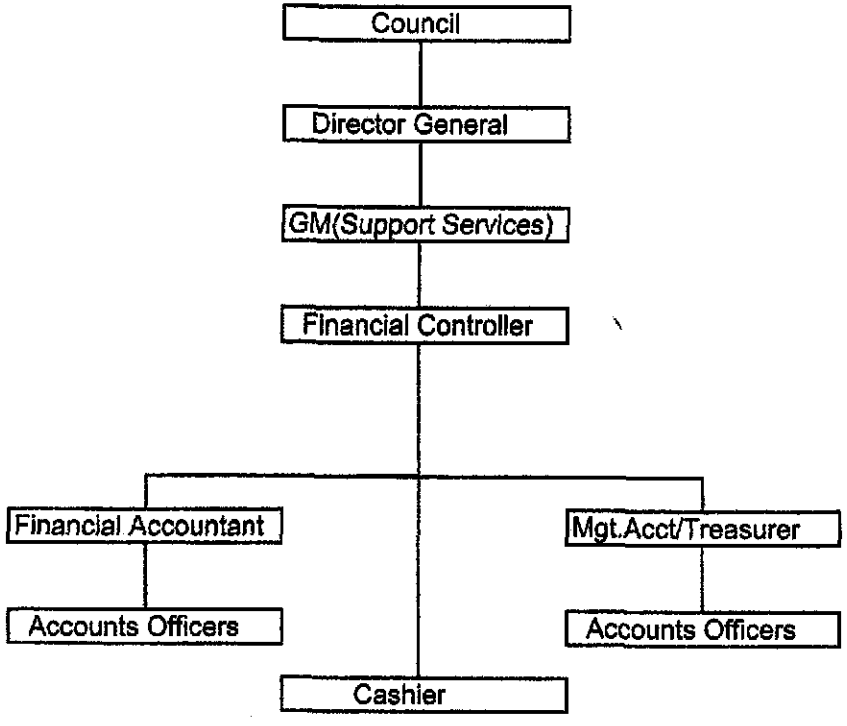
THE NIGERIAN STOCK EXCHANGE

HUMAN RESOURCE/ADMIN SECTION
PROPOSED ORGANIZATION CHART



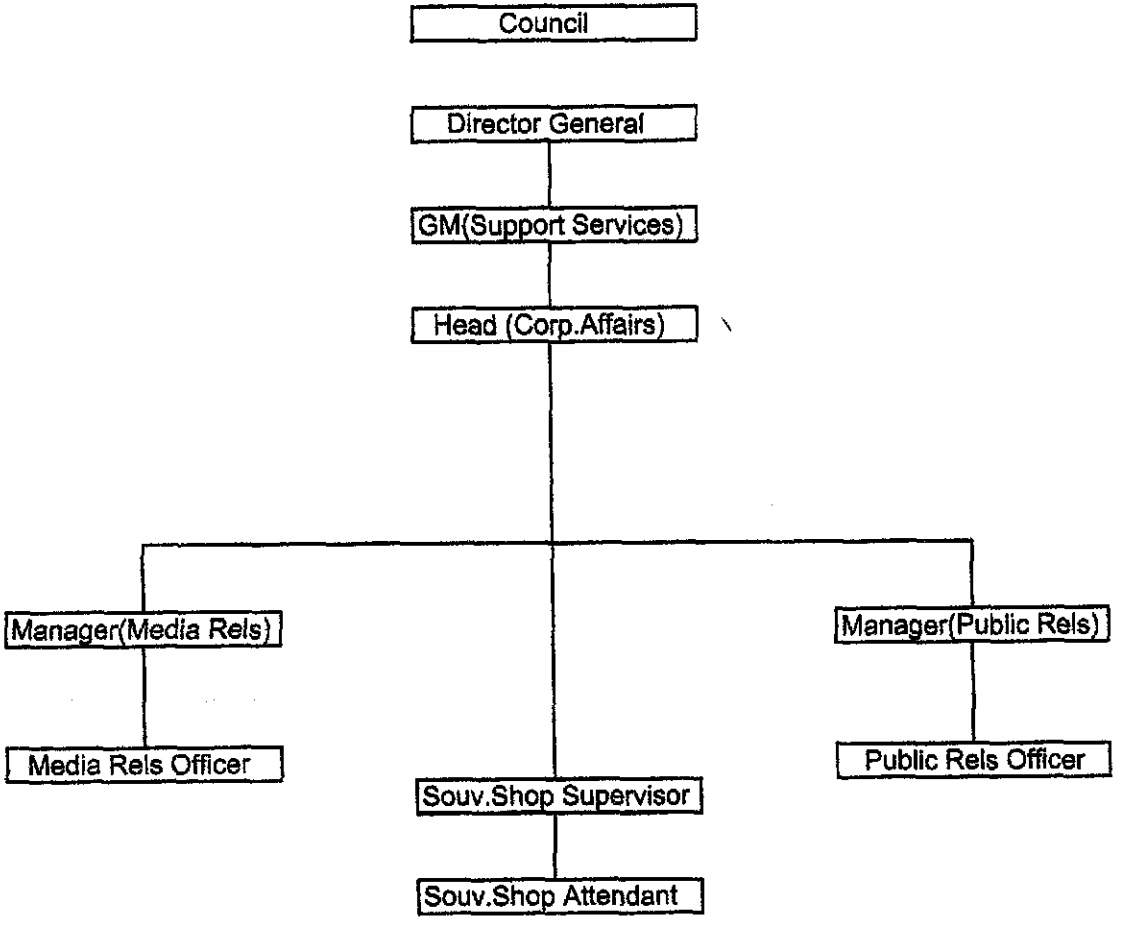
THE NIGERIAN STOCK EXCHANGE

FINANCE / ACCOUNTS SECTION
PROPOSED ORGANIZATION CHART



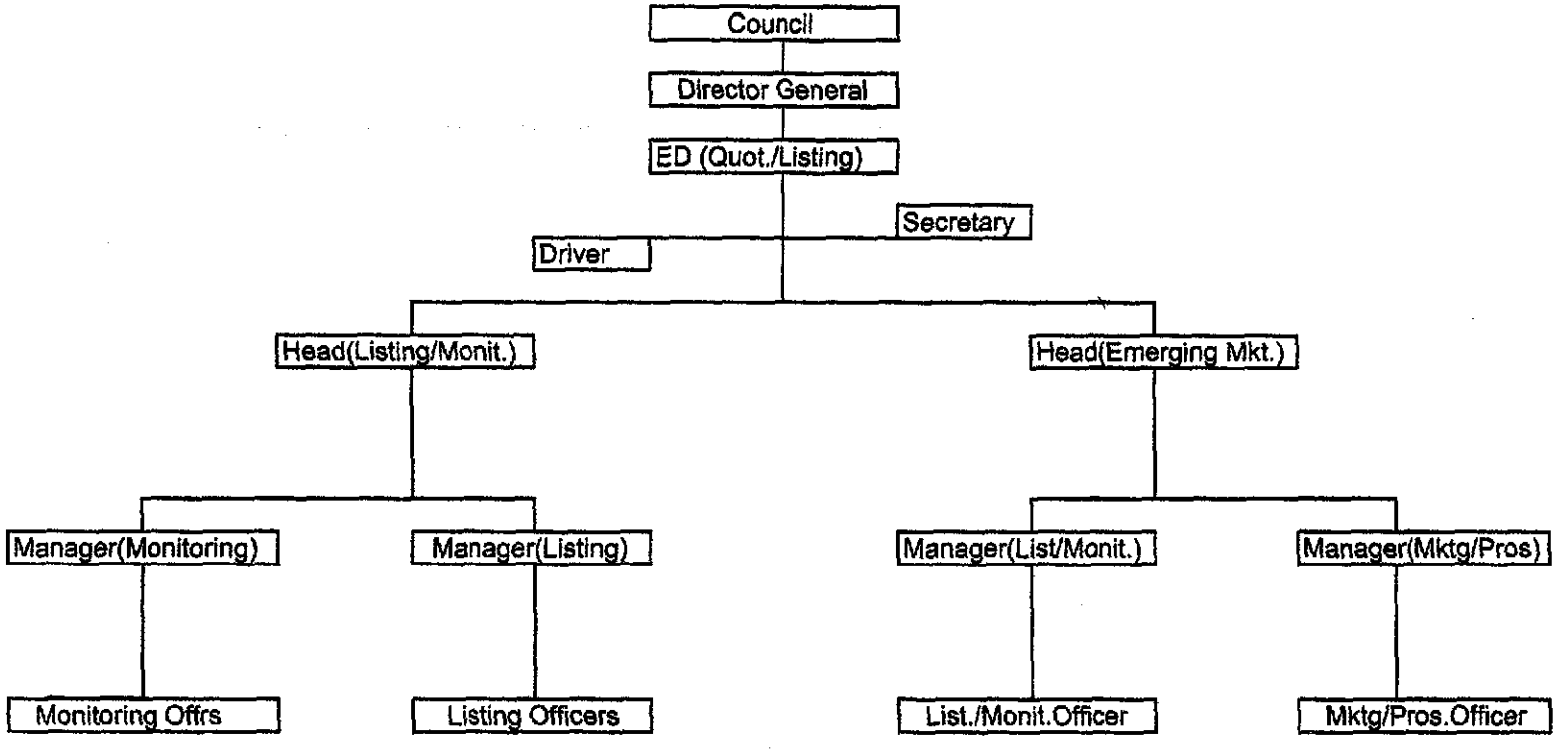
THE NIGERIAN STOCK EXCHANGE

CORPORATE AFFAIRS SECTION
PROPOSED ORGANIZATION CHART



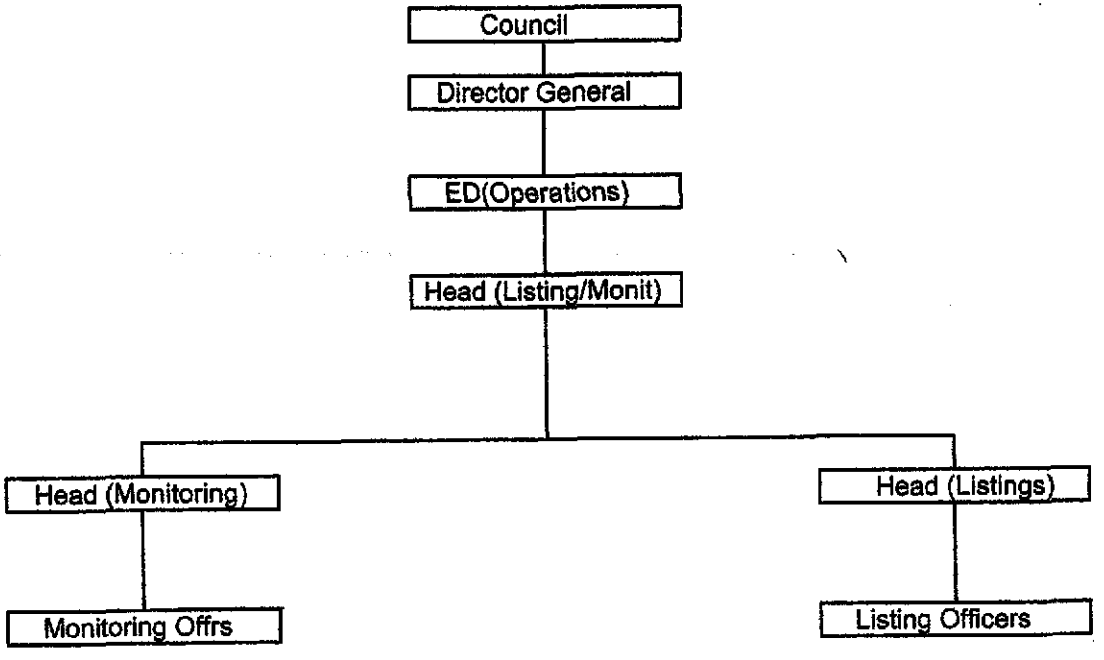
THE NIGERIAN STOCK EXCHANGE

QUOTATION / LISTING DIVISION
PROPOSED ORGANIZATION CHART



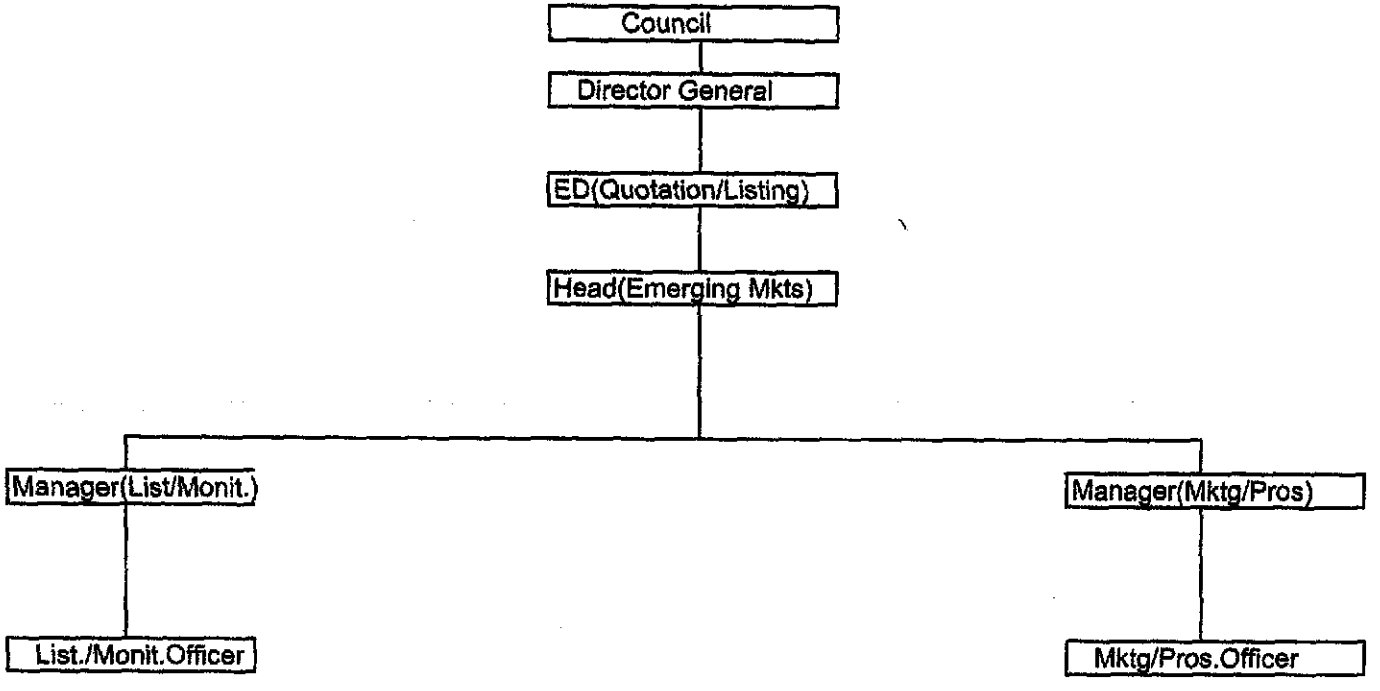
THE NIGERIAN STOCK EXCHANGE

LISTING & MONITORING DEPARTMENT
PROPOSED ORGANIZATION CHART



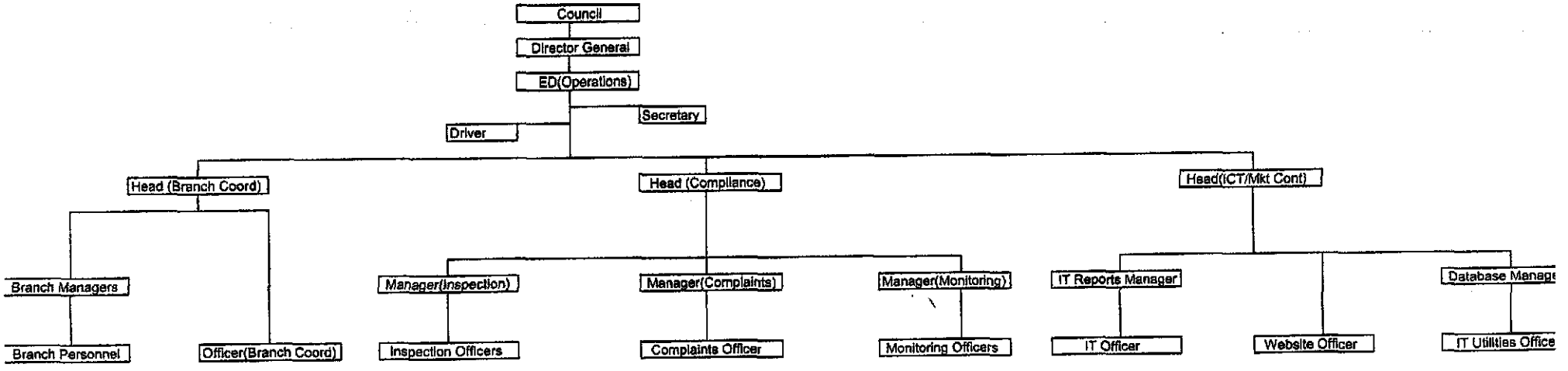
THE NIGERIAN STOCK EXCHANGE

EMERGING MARKETS DEPARTMENT
PROPOSED ORGANIZATION CHART



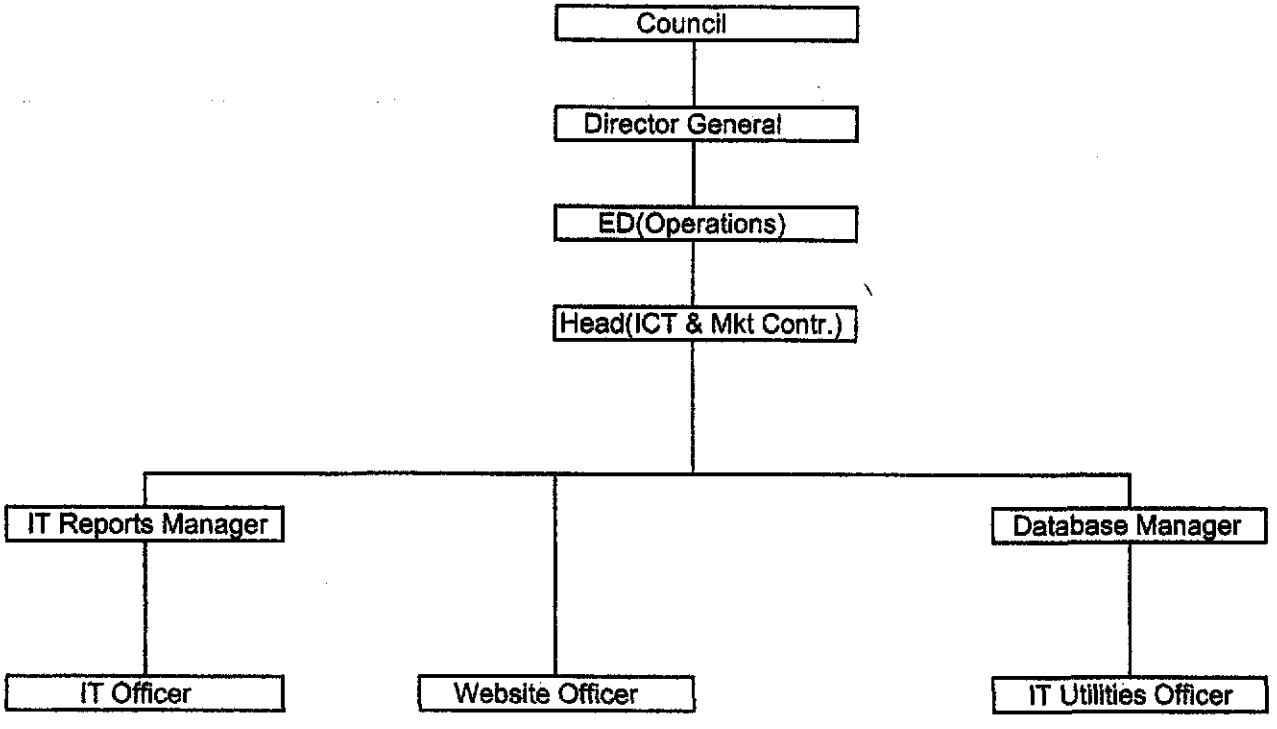
THE NIGERIAN STOCK EXCHANGE

OPERATIONS DIVISION
PROPOSED ORGANIZATION CHART



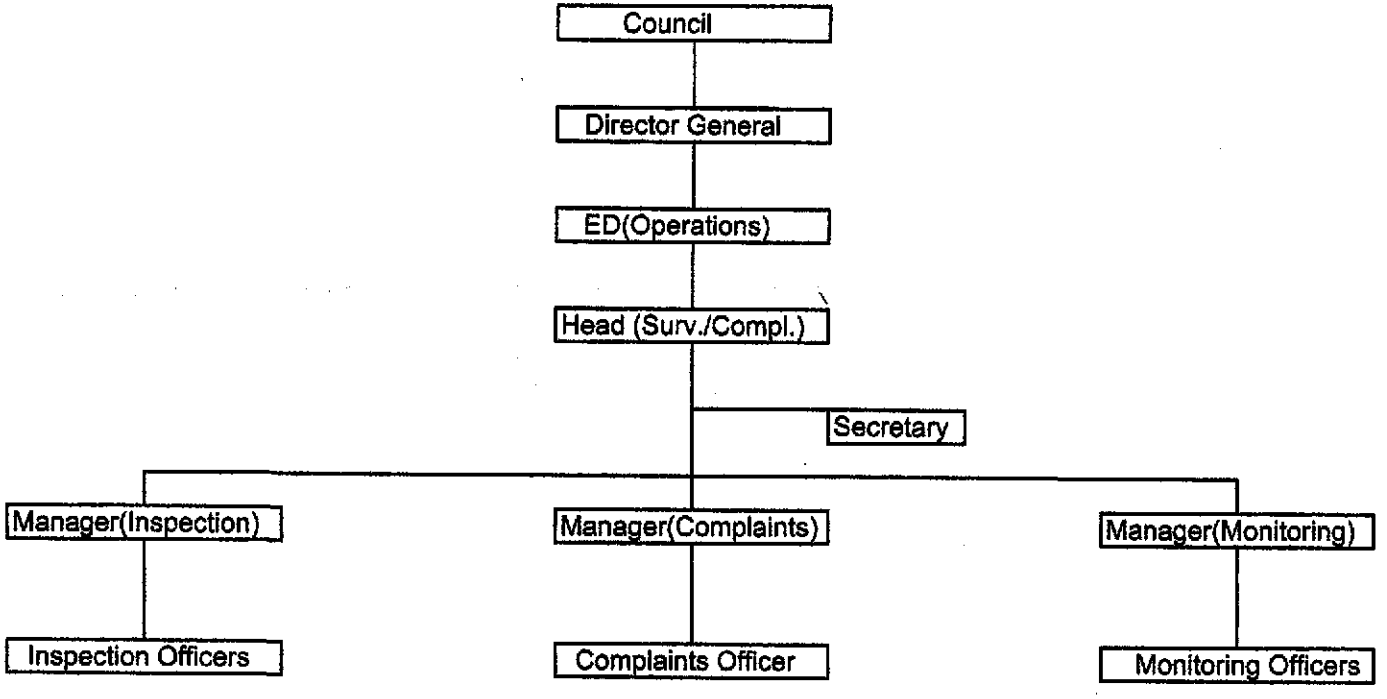
THE NIGERIAN STOCK EXCHANGE

INFOTECH & MARKET CONTROL DEPARTMENT
PROPOSED ORGANIZATION CHART



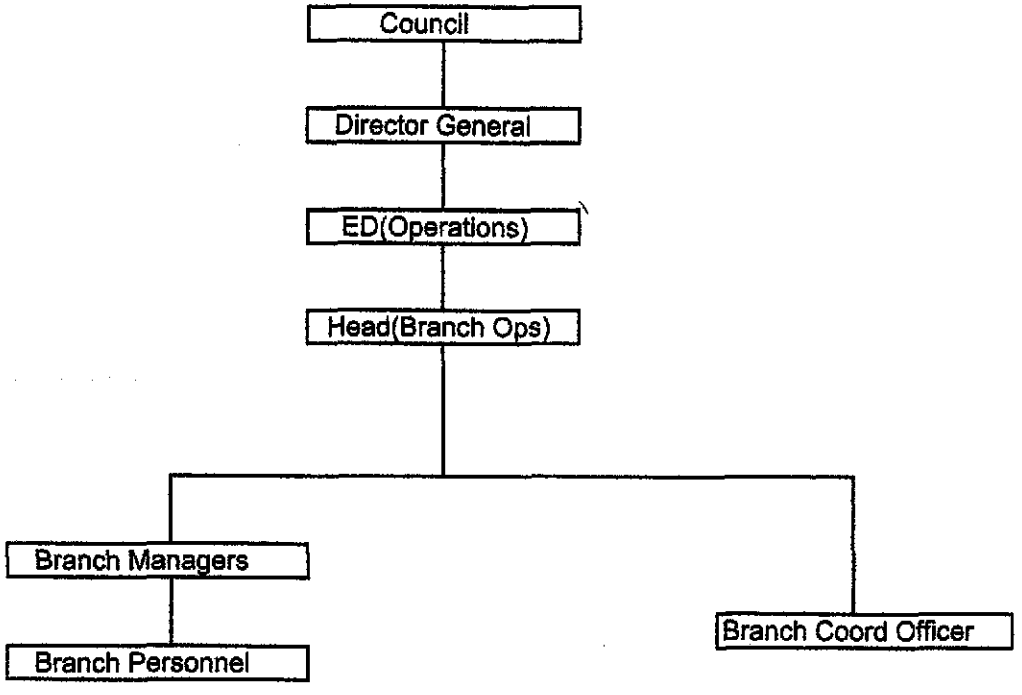
THE NIGERIAN STOCK EXCHANGE

SURVEILLANCE/COMPLIANCE DEPARTMENT
PROPOSED ORGANIZATION CHART



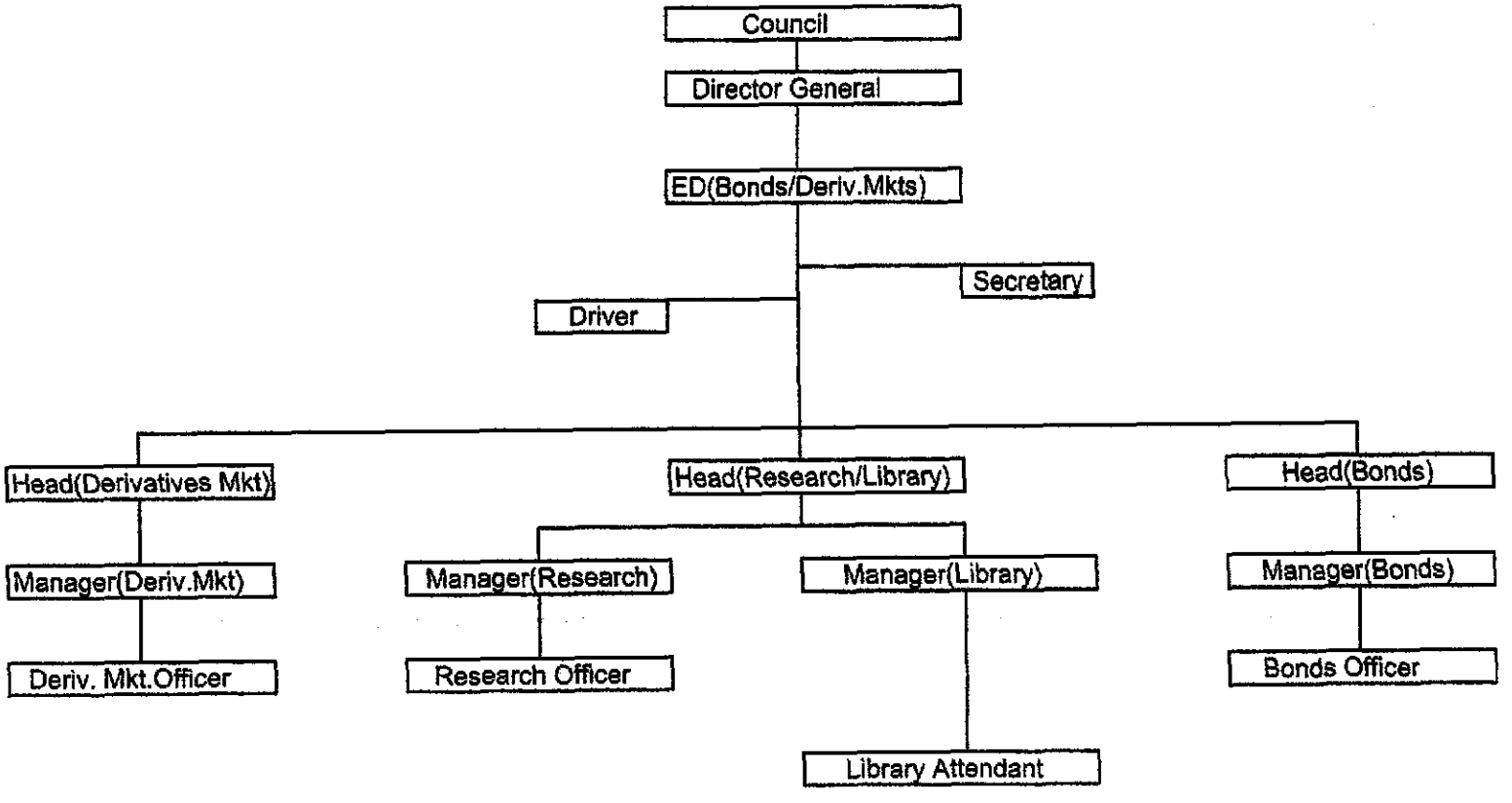
THE NIGERIAN STOCK EXCHANGE

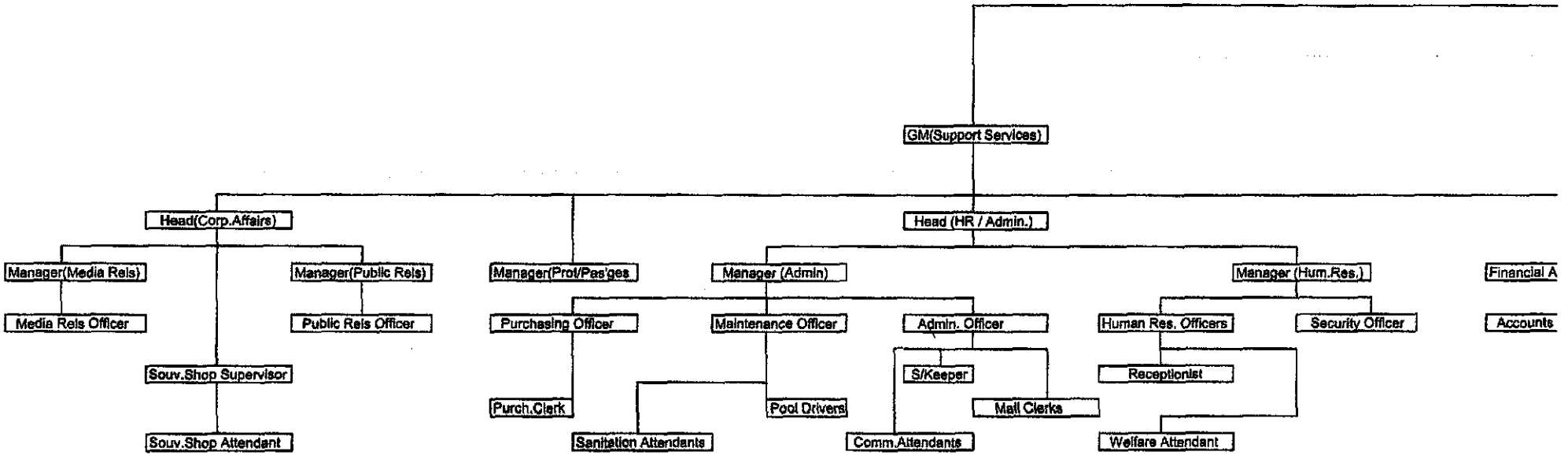
BRANCH OPERATIONS SECTION
PROPOSED ORGANIZATION CHART



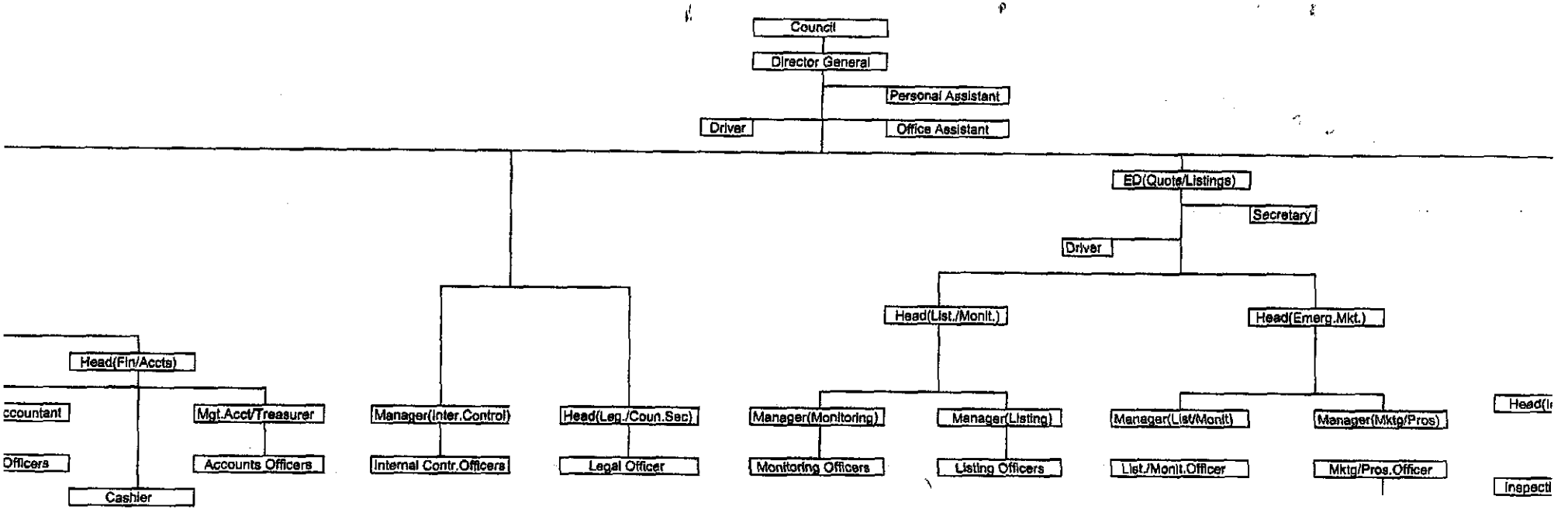
THE NIGERIAN STOCK EXCHANGE

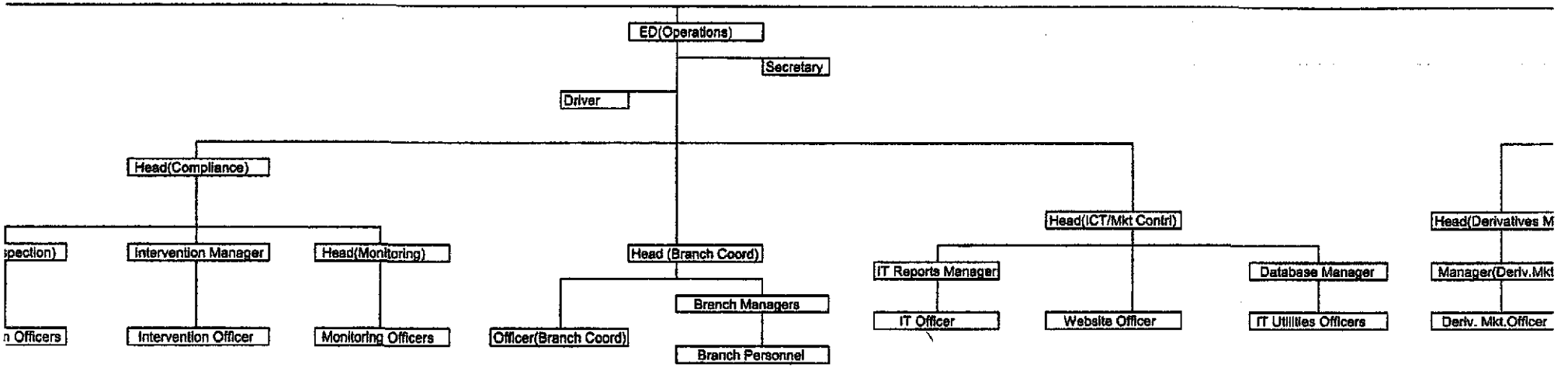
BONDS/DERIVATIVES MARKETS DIVISION
PROPOSED ORGANIZATION CHART

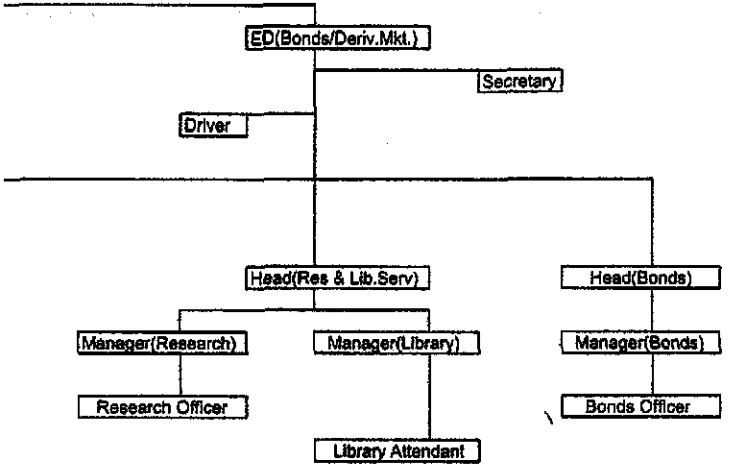



GM(Support Services)
Head(Corp.Affairs)
Head (HR / Admin.)
Manager(Media Rels)
Manager(Public Rels)
Manager(Prot/Pas'ges
Manager (Admin)
Manager (Hum.Res.)
Financial A
Media Rels Officer
Public Rels Officer
Purchasing Officer
Maintenance Officer
Admin. Officer
Human Res. Officers
Security Officer
Accounts
Souv.Shop Supervisor
S/Keeper
Receptionist
Purch.Clerk
Pool Drivers
Mail Clerks
Souv.Shop Attendant
Sanitation Attendants
Comm.Attendants
Welfare Attendant

THE NIGERIAN STOCK EXCHANGE
PROPOSED ORGANIZATION CHART




ED(Operations)
Secretary
Driver
Head(Compliance)
Head(ICT/Mkt Contrl)
Head(Derivatives M
spection)
Intervention Manager
Head(Monitoring)
Head (Branch Coord)
IT Reports Manager
Database Manager
Manager(Deriv.Mkt
Branch Managers
n Officers
Intervention Officer
Monitoring Officers
Officer(Branch Coord)
IT Officer
Website Officer
IT Utilities Officers
Deriv. Mkt.Officer
Branch Personnel


ED(Bonds/Deriv.Mkt.)
Secretary
Driver
Head(Res & Lib.Serv)
Head(Bonds)
Manager(Research)
Manager(Library)
Manager(Bonds)
Research Officer
Bonds Officer
Library Attendant

APPENDIX 16

16. NSE BCP/DRP Project Questionnaire Response

Appedix Details begin on Next Page

NSE BCP/DRP Project

QUESTIONNAIRE

THE Nigerian STOCK EXCHANGE

Your Name:	OSITA OLIBONNAYA	**Title:**	DEPUTY GEN. MGR IT & MKT Operations
Job Function	INFORMATION TECH & MARKET OPERATIONS	**Reports to:**	GM/HEAD IT & MKT Operations
Date:	30-11-2009		30-11-2009

Background

This Questionnaire Guide is used to determine your input into the NSE Disaster Recovery Planning & Business Continuity Planning project.

The DRP will provide a mechanism for continuous trading and support of the NSE in case of failure of the main building or main equipment and ensure that the data stored and transferred on the NSE's hardware and communications infrastructure is fully recoverable and secure.

The Technical Assistance will include the review of existing IT systems and plans, existing hardware and communications infrastructure, and would develop a strategic plan, specifications, and an implementation plan for a disaster recovery facility. The Technical Assistance will also ensure that any recommended procurements can be integrated with existing hardware, communications infrastructure, applications, and databases.

The data gathered will form the basis for comparison to industry-based Disaster Recovery Planning Best Practices. A Gap Analysis will be documented as a critical component of the "NSE DR As-Is Assessment" delivered to NSE.

GIT will utilize the Gap Analysis and DR Assessment along with the DR Best Practices and its extensive experience to develop and document the critical procedures, forms and reports that will be integrated into an overall NSE DR Facility Development Plan.

This Guide is made up of a number of questions in five (5) broad areas pertaining to information that we have found to be important to the successful implementation of the NSE DRP. These include:

- **Current NSE Environment**
- **NSE Emergency Response Procedures**
- **NSE DR Plan Activation Procedures**
- **NSE Administrative Procedures**
- **NSE DR Reports & Forms**

mts

NSE BCP/DRP Project

QUESTIONNAIRE

At the end of each section is an area to provide any general Comments that you may have about the overall section.

GENERAL INSTRUCTIONS

Enter the information that "best" represents your specific understanding about the Disaster Recovery and Business Continuation needs for NSE. Add extra information wherever necessary – attach any information requested.

If you create a "soft-copy," create a "Save As" copy using your Initials and the date. For Example: IB-2-20 NSE Q v 1.0"

CIRCLE your answer to each question. Please do not guess: if you don't know the answer, don't respond to the question. Keep in mind that you can identify that you "Don't Know" (DK) for any question area(s) that do not apply to your job, or where you have no direct information.

Please enter as much clarifying information as you can.

Note: All of the information entered this questionnaire will be held in strict confidence.

PLEASE RETURN THE COMPLETED GUIDE FILE WITHIN ONE WEEK AFTER YOU RECEIVE IT

Next Steps:

1. **Complete the Questionnaire and return both paper AND "soft"-copy)**
2. **The GIT project team will consolidate Results**
3. **The GIT project team will Report back to You and all Stakeholders with a draft DRP**
4. **The GIT project team will develop the final DRP and present to NSE**
5. **The GIT project team will continue to work with you.**

If you have any questions, please call or contact:

- **Mike Ike 901-218-6233 or**
- **Irv Brownstein at 908-872-8139.**

MB

NSE BCP/DRP Project

QUESTIONNAIRE

Thank You!!

mts

NSE BCP/DRP Project

QUESTIONNAIRE

THE Nigerian STOCK EXCHANGE

CURRENT NSE ENVIRONMENT

	Is there an NSE Disaster Recovery (DR) POLICY Statement? YES or NO or DK (Don't Know) NO
	If YES, Please Attach N/A

	Is there a current DR PLAN? YES or NO or DK NO
	If YES, Please Attach N/A

Identify the INDIVIDUALS to be contacted In case of emergency N/A

Immediately Notify The Key Emergency Contacts Listed Below:

Contact	Office Number	Home / Mobile Phone
Security Desk		

In the event that none of the above key contacts are available, call

Who must APPROVE the Disaster/Recovery Plan? List All individuals

Name	Title/Function
Prof Ndi Okereke Onyiuke	Group MD / CEO
Mr. Binos Yaroe	GM / Head, Information Tech & Operations
Mr. Taba Peterside	GM (Head) Risk Mgt & Regulation
Mr. Osita Ogbonnaya	DGM, Information Tech & Mkt Ops

NSE BCP/DRP Project

QUESTIONNAIRE

THE NEW YORK STOCK EXCHANGE

Is there a FAIL-OVER SITE? YES or NO or DK

If Yes, Do you have a current Fail-Over site agreement? (ATTACH)

Date executed? NO

Does the Fail-over site have the same

- Software? YES or NO - IF YES, ATTACH LIST
- Supplies? YES or NO IF YES, ATTACH LIST

Has the Site been tested in a formal fire-drill? YES or NO

- If YES, When? NO
- IF YES, What results? (ATTACH RESULTS) NONE

What are the current NSE processing VOLUMES?

For each Transaction type – identify the Volume, Period, Peak period volumes

Identify the general volume history over the past 24 months (or attach separate report covering the same data).

Month	Daily Volume	Peak Volume (hours)	Comment
	SEE ATTACHED		

Identify the failure history over the past 18 months. In each case detail each outage using the following table (or attach separate report covering the same data).

NSE BCP/DRP Project

QUESTIONNAIRE

THE NIGERIAN STOCK EXCHANGE

Date	Duration	Impact/Extent	Cause / Comment

NO PLAN IN PLACE TO DOCUMENT THIS INFORMATION

Identify the KEY CONTACT INFORMATION related to each critical business function? List All individuals

Function Name	Name & Title/& Contact Information

NOT CLEARLY DEFINED FOR NOW

List all software used to support NSE (List Below Or Attach Report)

Name	Vendor/supplier	Version/release	Use

Identify the current NETWORK for both data and telecommunications

Provide one or more systems architecture chart(s) that highlights each element of the

- IT Infrastructure depicting each device type
- Telecommunications protocols

mts

NSE BCP/DRP Project

QUESTIONNAIRE

THE Nigerian STOCK EXCHANGE

	Describe BUSINESS UNIT INVOLVEMENT with the NSE DR
	How many people are involved from your business units in BCP planning? NONE
	Are they accountable for plan content development and approval? NO
	Do they participate in testing exercises? NO

	Describe NSE SECURITY related to the NSE DR
	Do you have fulltime security personnel? YES
	Are they included in your BC/DR plans?
	Have you defined predefined roles during an outage? NO

	Identify the NSE EXECUTIVE SPONSORSHIP
	Who is responsible for Business Continuity Planning?
	What is the organizational structure? UNDER DEVELOPMENT
	Do you have a steering committee of representatives? NO
	How frequently do they review plan readiness and issues? NONE
	If you have a board of directors, is BCP reviewed? NO

	Describe NSE RISK ASSESSMENT
	Do you perform routine facility risk assessments? NO
	Do you meet with local fire, police, and Hazardous Material teams to ensure assumptions in plan are within their guidance? NO
	Have you identified internal and external threats? NOT YET

mts

NSE BCP/DRP Project

QUESTIONNAIRE

	Do you have controls in place to monitor Security, Life Safety, and Communication to Personnel? NO
	Have you developed risk exposures and financial cost analysis? NOT YET

COMMENTS:

mts

NSE BCP/DRP Project

QUESTIONNAIRE

THE Nigerian STOCK EXCHANGE

NSE EMERGENCY RESPONSE PROCEDURES

Emergency response ensures that all parties act to quickly determine the emergency and take appropriate action. GIT will complete this stage of the project in three tasks:

- Emergency Evacuation Procedures
- Emergency Phone Numbers
- Emergency Notification Procedures.

A business disruption has three distinct phases: Emergency, Recovery, and Restoration. The emergency operations center (EOC) is the focal point of communication and coordination for resources during a business disruption.

	Is there an EMERGENCY MANAGEMENT TEAM? YES or NO or DK
	If YES Please describe or attach NO

	Is there an EMERGENCY OPERATION CENTER? YES or NO or DK
	If YES Please describe or attach NO

	Are there documented EMERGENCY PROCEDURES? YES or NO or DK
	If YES is there a chart that outlines the procedure steps that address notification and mobilization (Please attach)? NO
	Identify in the table below (or attach) the procedures that indicate what steps are followed AND who (Name & Title) is responsible for the specific actions. NO EMERGENCY PROCEDURE AVAILABLE YET.

Step	ACTION/PROCEDURES	WHO
1		
2		
3		

mtp

NSE BCP/DRP Project

QUESTIONNAIRE

THE Nasdaq STOCK EXCHANGE

Identify the current NSE EMERGENCY CONTACT LIST

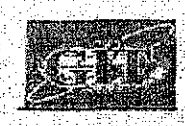
Notified By	EMT Role	EMT Member Name	Numbers
	EMT Leader		

H = home W = work C = cellular S = satellite F = fax

NOT AVAILABLE

COMMENTS:

mto



NSE BCP/DRP Project

QUESTIONNAIRE

NSE DR PLAN ACTIVATION PROCEDURES

Plan activation ensures that all parties and all materials are coordinated for the DR Facility. GIT will complete this stage of the project in ten (10) tasks:

- Activate Incident Management Team
- Activate Emergency Operations Center
- Emergency Declaration Procedures
- Relocate Operations Procedures
- Situation & Damage Assessment Procedures
- Communications
- Offsite Storage
- Purchasing procedures
- Recovery Site Generator, Electrical & Security plan Procedures
- Reconstruction Procedures

Identify the Mission CRITICAL BUSINESS FUNCTIONS AND PROCESSES

For each critical function service, product and/or system identify the time-frame (Notification and Recovery) that it must be fully operational (Note: use additional pages as necessary)

Critical Business System Function/Process	Recovery Time Objective
	Notification: Recovery:
	Notification: Recovery:
	Notification: Recovery:
	Notification: Recovery:
	Notification: Recovery:

Note: All recovery time objectives, other than immediate, reflect business days or weeks.

mts

NSE BCP/DRP Project

QUESTIONNAIRE

THE Nigerian STOCK EXCHANGE

Are there RECOVERY STRATEGIES Associated With All Or Any Business Segment Or Function? YES or NO NO

I. TRANSFER OF WORK	
Approach	Responsibility
II. IN HOUSE RECOVERY	
Approach	Responsibility
III. WORK FROM HOME	
Approach	Responsibility

Is there a defined RECOVERY ORGANIZATION? YES or NO NO

If YES Please describe or attach

Name	Function

If YES, what are their ROLES AND RESPONSIBILITIES (Describe or attach)

Function	Role	Responsibilities

NSE BCP/DRP Project

QUESTIONNAIRE

THE Nigerian STOCK EXCHANGE

This section identifies the specific procedures for Disaster Recovery Teams to follow during the various stages of a disaster. NOT AVAILABLE

Identify and describe the Procedure Steps for the EMERGENCY PHASE (or attach)

Identify in the table below (or attach) the procedures that indicate what steps are followed AND who (Name & Title) is responsible for the specific actions.

Step	ACTION/PROCEDURES	WHO
1		
2		
3		

Identify and describe the Procedure Steps for the RECOVERY PHASE (or attach) N/A

Identify in the table below (or attach) the procedures that indicate what steps are followed AND who (Name & Title) is responsible for the specific actions.

Step	ACTION/PROCEDURES	WHO
1		
2		
3		

Identify and describe the Procedure Steps for the RESTORATION PHASE (or attach) N/A

Identify in the table below (or attach) the procedures that indicate what steps are followed AND who (Name & Title) is responsible for the specific actions.

mto

NSE BCP/DRP Project

QUESTIONNAIRE

THE NIGERIAN STOCK EXCHANGE

Step	ACTION/PROCEDURES	WHO
1		
2		
3		

Identify the RESOURCES - Software, Hardware and Supplies associated with the procedures

Include (or attach) references to space, specific supplies, software names and versions, hardware devices

Item	Description and Use

COMMENTS:

mts

NSE BCP/DRP Project

QUESTIONNAIRE

THE Nigerian STOCK EXCHANGE

NSE ADMINISTRATIVE PROCEDURES

The administrative responsibilities summarize NSE policy. These responsibilities and procedural guidelines must be applied throughout the initial response and any subsequent business recovery activities.

- Enforce NSE Policies
- Monitor & Report Recovery process
- Maintain Recovery Related Record Keeping
- Define Testing & Maintenance Functions

Is There A Defined MAINTENANCE SCHEDULE (Describe Below Or Attach)? YES or NO or DK NOT COMPREHENSIVE – ONLY FOR SOME IT & BUILDING EQUIPMENT

What Events Trigger A MAINTENANCE REVIEW? ANY THING BECAUSE OF LACK OF STRUCTURED APPROACH TO PROBLEM RESOLUTION

The following table includes many events that may necessitate a maintenance review.

Situation	Actions Taken

Are DISASTER RECOVERY PLAN UPDATES Made On A Scheduled Basis? YES or NO or DK NO PLAN YET

Yes – Describe And Identify The Distribution

Are there DIRECTIONS to Emergency Operations Centers? YES or NO or DK NO

MTP

NSE BCP/DRP Project

QUESTIONNAIRE

THE Nigerian STOCK EXCHANGE

	How are Policies ENFORCED? (Describe Below Or Attach)
	NO POLICIES IN PLACE YET

	How is Record Keeping MAINTAINED? (Describe Below Or Attach)?
	MANUALLY ON FILES & CABINETS FOR NOW

	Is there a DAMAGE ASSESSMENT CHECKLIST? (See Sample) YES or NO or DK
	If Yes – Describe or attach NONE YET

	Is there a FACILITIES EMERGENCY PROCEDURES? YES or NO or DK
	If Yes – Describe or attach NONE YET

	Is there an ORGANIZATION CHART with a Master Employee Listing? YES or NO or DK
	If Yes – Describe or attach YES BUT A NEW ONE IS IN DEVELOPMENT
	How frequently is your call tree updated? NOT YET AVAILABLE

	Is there a RECOVERY STATUS REPORT? (See Sample) YES or NO or DK NO
	If Yes – Describe or attach

NSE BCP/DRP Project

QUESTIONNAIRE

THE Nigerian STOCK EXCHANGE

Is there an APPROVED PRESS RELEASE? (See Sample) YES or NO or DK

If Yes – Describe or attach NO

Is there a MAINTENANCE LOG? YES or NO or DK

If Yes – Describe or attach ONLY FOR SOME IT EQUIPMENTS. BACKUP GENERATORS AND OFFICE EQUIPMENT. BUT FORMAL LOG BOOK IN PLACE

Describe the NSE Profile

How long has NSE been in business? 49 YEARS

How many locations does NSE have? What is the number of people by location? 20+ Branches 1 HQ

How many people are within NSE overall? ≈ 300

Please define the organizational structural by business unit? STILL IN DEVELOPMENT

What percent of the NSE budget is dedicated towards BCP? NONE

Does NSE currently have a BCP Steering Committee? NO

Who are NSE's primary client(s)? Where are they located? BROKERS, LISTED COYS, GOVERNMENT REGULATORS, BANKS, REGISTRARS, PUBLICS, FOREIGN INVESTORS. GLOBALLY LOCATED

How is Client COMMUNICATION handled about NSE "Disasters"?

What is communicated to your clients concerning BCP? NOTHING

Do you track what was said and to whom? NO

NSE BCP/DRP Project

QUESTIONNAIRE

THE NIGERIAN STOCK EXCHANGE

	How is Client COMMUNICATION handled about NSE "Disasters"?
	Do you receive inquiries from clients? SOMETIMES
	Do clients ask for onsite visits? NO
	Do you have a centralized repository for issue management? NO
	Who is overseeing closure of critical issues? VARIOUS UNITS
	Do you utilize any tools for mass communication? Do you utilize your website?
	How do you to communicate to personnel during a situation? BY PHONE
	How frequently do you communicate plans status, evacuation plans, and life safety preparedness to your personnel? RARELY
	Do you have a plan to communicate to external vendors and clients? Have you tested this? When and What was the result? NONE YET

	Identify the NSE DR PROGRAM CONTROLS
	How do you monitor your plan readiness? N/A
	What metrics do you use for testing of plan content? NONE YET
	What percent of people participate in business unit testing? NONE
	Do you review your program with Legal/Compliance teams? N/A

	Discuss NSE DR PROGRAM MATURITY
	Have you instituted a firm-wide plan for business continuity? NO
	Are key members of your businesses involved? NONE YET
	What percent of BCP activities are completed with Information Technology? DATA BACKUP ONLY

	Describe NSE LIFE SAFETY related to the NSE DR

NSE BCP/DRP Project

QUESTIONNAIRE

THE Nigerian STOCK EXCHANGE

	Do you have first aid responders within your buildings? NO
	What is the frequency of their training? NONE
	Do you personnel know who they are and how to engage with them? NO
	Do you they have role within the Incident Management Plan? NONE YET

	Describe NSE INCIDENT MANAGEMENT PROGRAM related to the NSE DR
	Do you include life safety, security, business units, and IT in your incident management program?
	Do you have a location near the building for people to gather in a evacuation? NO
	Do you have a mechanism to verify all people have safely left the building? NO
	Do you have a Incident Manager for each site in your organization? NO
	Do you have a checklist for that person to execute and provide status? NONE
	Have roles and responsibilities been clearly assigned for during the event? NO

	Describe NSE INDUSTRY TESTING related to the NSE DR
	Do you participate in industry testing? NO
	Do you test with your critical vendors? YET TO START
	What level of participation is required? NOT KNOWN YET
	How frequently do you test? NO TESTING CARRIED OUT YET

	Describe NSE BACKUP SITE INVOCATION PLANS related to the NSE DR
	Do you have steps to activate your backup site? YES BUT LIMITED IN SCOPE
	Do they include communication, transportation, and logistics? YES

MLO

NSE BCP/DRP Project

QUESTIONNAIRE

	Do you have decision points contained in the plan? NO DOCUMENTED PLAN YET

COMMENTS:

MB

NSE DR REPORTS AND FORMS

The Reports are a critical mechanism for communication throughout and after the Disaster/Recovery period.

- Business Unit Key Contacts
- Summary of Critical Applications, Servers & Recovery Time Objectives (RTOs)
- Vendors & Suppliers
- Summary of Desktop & Workspace Requirements
- Other Equipment
- Critical Telephone Numbers Report

N/A

The Forms are a critical support provided to all Recovery Teams for use throughout and after the Disaster/Recovery period.

- Recovery Activities Log
- Critical Files & In-Progress Assessment
- Critical Equipment & Assessment
- Personnel Locations Control Form
- Time Sheet tracking
- Telephone Log
- Damage Control Status
- Bomb Threat Response
- Injury Status Reporting
- Receiving Room Sign-In

N/A

	Are the following key DR REPORTS used by NSE? YES or NO or DK for each
	If Yes – Describe And Identify The Distribution – Attach a SAMPLE The Reports are a critical mechanism for communication throughout and after the Disaster/Recovery period. • Business Unit Key Contacts NO • Summary of Critical Applications, Servers & Recovery Time Objectives (RTOs) NO

nts

NSE BCP/DRP Project

QUESTIONNAIRE

THE Nigerian STOCK EXCHANGE

Are the following key DR REPORTS used by NSE? YES or NO or DK for each
• Vendors & Suppliers • Summary of Desktop & Workspace Requirements • Other Equipment • Critical Telephone Numbers Report

N/A

Are the following key DR FORMS used by NSE? YES or NO or DK for each
If Yes – Describe And Identify The Distribution – Attach a SAMPLE The Forms are a critical support provided to all Recovery Teams for use throughout and after the Disaster/Recovery period. • Recovery Activities Log • Critical Files & In-Progress Assessment • Critical Equipment & Assessment • Personnel Locations Control Form • Time Sheet tracking • Telephone Log • Damage Control Status • Bomb Threat Response • Injury Status Reporting • Receiving Room Sign-In

N/A

NSE BCP/DRP Project

QUESTIONNAIRE

THE Nigerian STOCK EXCHANGE

Describe NSE DATA STORAGE related to the NSE DR Data	
Do you currently backup your servers?	YES BUT HIGHLY INADEQUATE
Do you utilize a third party for this service?	NO
Have you reviewed their BCP plan?	N/A
Did this meet or exceed your requirements for service?	N/A
What medium is utilized for this function?	N/A
How frequently is this completed?	
Have you successfully tested recovering this data at an alternative location?	
Did this test meet or exceed your recovery objectives?	

Describe NSE VITAL RECORDS related to the NSE DR	
Have you inventoried your critical records?	NOT QUITE
Have you secured offsite storage?	NO
What percent of records are remaining onsite?	N/A
How frequently do you send offsite?	
Have you visited the site as part of due diligence?	
Have you tested that you could retrieve critical records in the time stated in service level agreement?	

COMMENTS:

MEO

NSE BCP/DRP Project

QUESTIONNAIRE

THE Nigerian STOCK EXCHANGE

APPENDIX 17

17. GIT NSE DRP Proposal for Technical Assistance

NIGERIAN STOCK EXCHANGE DISASTER RECOVERY AND SYSTEMS BACKUP PROJECT TECHNICAL ASSISTANCE

Prepared for:

U.S. TRADE AND DEVELOPMENT AGENCY
1000 Wilson Boulevard
Arlington, VA 22209

Prepared by:

GLOBAL INFORMATION TECHNOLOGY INC.
8913 Regents Park Drive
Suite #880
Tampa, FL 33647

11 August 2006

VERSION 1.0

Appedix Details begin on Next Page

NIGERIAN STOCK EXCHANGE DISASTER RECOVERY AND SYSTEMS BACKUP PROJECT TECHNICAL ASSISTANCE

Prepared for:

U.S. TRADE AND DEVELOPMENT AGENCY
1000 Wilson Boulevard
Arlington, VA 22209

Prepared by:

GLOBAL INFORMATION TECHNOLOGY INC.
8913 Regents Park Drive
Suite #880
Tampa, FL 33647

11 August 2006

VERSION 1.0

TABLE OF CONTENTS

1.0 SECTION ONE: INTRODUCTION AND EXECUTIVE SUMMARY *6*

1.1 Background **6**

1.2 Work to Be Accomplished **6**

1.3 DRP Stages & Tasks **7**

DR Data Gathering & Current State Assessment 7
Document DR Emergency Response Procedures 7
Document DR Plan Activation Procedures 7
Document Administrative Procedures 8
Document Key DR Reports 8
Document Key DR Forms 8
Final Delivery & Reporting 8

1.4 DRP Deliverables **9**

1.5 The GIT Team **10**

2.0 SECTION 2: COMPANY INFORMATION *11*

2.1 Company Profile **11**

2.2 Company Philosophy **11**

2.2 Offeror's Authorized Negotiator **12**

2.3 Negotiation Prerequisites **13**

Authorization and Approval 13

3.0 SECTION 3: ORGANIZATIONAL STRUCTURE, MANAGEMENT, AND KEY PERSONNEL *15*

3.1 Organizational Structure **15**

GIT Management Organization chart 15

3.2 Delivery Management Team **15**

GIT Delivery Director 15
GIT Project Manager 19

GIT Project Management Philosophy **24**

Project Management Approach **25**

Project Monitoring **26**

Project Reporting **26**

Project Control **26**

Management Review 26
Project Management Meetings 26
Project Steering Committee 27
Problem Resolution 27
Risk Management 27
Change Management 27
Change Initiation 27
Change Validation 28
Cost Estimate Preparation 28
Change Approval 28
Change Implementation 28
Quality Management Process 28
Quality Control 29
Quality Assurance 29

Quality Review Process 29

3.3 Key Personnel **30**

3.4 Project Monitoring and Status Reporting **30**

4.0 SECTION 4: TECHNICAL APPROACH AND WORK PLAN ***31***

4.1 Overview and Background **31**
4.1.1 Scope 31
4.1.2 Current NSE Business & Environment 31
4.1.3 Work Approach 33

4.2 DR Data Gathering & Current State Assessment **34**
4.2.1 Identify key Areas/individuals 34
4.2.2 Distribute/Conduct Data Gathering Template(s) 34
4.2.3 Complete Gap Analysis & DR Assessment 34

4.3 Document DR Emergency Response Procedures **35**
4.3.1 Emergency Evacuation procedures 35
4.3.2 Emergency Phone Numbers 35
4.3.3 Emergency Notification Procedures 35

4.4 Document DR Plan Activation Procedures **35**
4.4.1 Activate Incident Management Team 36
4.4.2 Activate Emergency Operations Center (EOC) 36
4.4.3 Emergency Declaration Procedures 36
4.4.4 Relocate Operations Procedures 37
4.4.5 Situation & Damage Assessment Procedures 37
4.4.6 Communications 37
4.4.7 Offsite Storage 37
4.4.8 Purchasing procedures 38
4.4.9 Recovery Site Generator, Electrical & Security Plan Procedures 38
4.4.10 Reconstruction Procedures 38

4.5 Document DR Administrative Procedures **38**
4.5.1 Enforce NSE Policies 39
4.5.2 Monitor & Report Recovery process 39
4.5.3 Maintain Recovery Related Record Keeping 39
4.5.4 Define Testing & Maintenance Functions 39

4.6 Document Key DR Reports **39**
4.6.1 Business Unit Key Contacts 40
4.6.2 Summary of Critical Applications, Servers & RTO's 40
4.6.3 Vendors & Suppliers 40
4.6.4 Summary of Desktop & Workspace Requirements 40
4.6.5 Other Equipment 40
4.6.6 Critical Telephone Numbers Report 40

4.7 Document Key DR Forms **40**
4.7.1 Recovery Activities Log 41
4.7.2 Critical Files & In-Progress Assessment 41
4.7.3 Critical Equipment & Assessment 41
4.7.4 Personnel Locations Control Form 41
4.7.5 Time Sheet tracking 41
4.7.6 Telephone Log 41
4.7.7 Damage Control Status 41
4.7.8 Bomb Threat Response 41
4.7.9 Injury Status Reporting 42
4.7.10 Receiving Room Sign-In 42

4.8 Final Delivery & Reporting **42**
4.8.1 Develop DR Implementation Plan 42
4.8.2 Document & Deliver Final DR Report 42
4.8.3 Conduct Final DR Presentation 42

4.9 NSE DR Deliverables Summary & Schedule **42**

5.0 SECTION 5: EXPERIENCE AND QUALIFICATIONS *44*
5.1 Experience and Qualifications **44**
5.2 Project References **55**
6.0 SECTION 6: APPENDIX *57*
6.1 Disaster-Recovery Plan Data Gathering Template **57**
MANAGEMENT APPROVAL *59*
1. OVERVIEW **62**
1.1 POLICY STATEMENT **62**
1.2 SCOPE OF PLAN **62**
1.3 ASSUMPTIONS **62**
1.4 BUSINESS IMPACT ANALYSIS **62**
1.5 CRITICAL BUSINESS FUNCTIONS **62**
1.6 RECOVERY STRATEGIES **62**
1.7 PHASES OF RESPONSE **63**
1.8 RECOVERY ORGANIZATION **63**
1.9 ROLES AND RESPONSIBILITIES **63**
1.10 DISTRIBUTION POLICY **63**
2. EMERGENCY MOBILIZATION *63*
2.1 INTRODUCTION **63**
2.2 EMERGENCY OPERATIONS CENTER **63**
2.3 EMERGENCY MANAGEMENT TEAM **63**
2.4 EMERGENCY OPERATION CENTER PREPARATION **63**
2.6 EMERGENCY MANAGEMENT TEAM NOTIFICATION TREE **65**
EMT Member 65
3. TEAM ACTION PLANS *65*
3.1 EMERGENCY MANAGEMENT TEAM ACTION PLAN **65**
3.2 Mission Critical System - Template (1 per system) **66**
4. TESTING AND MAINTENANCE *69*
4.1 MAINTENANCE SCHEDULE **69**
4.2 EVENT TRIGGERED REVIEWS **69**
4.3 TESTING **69**
4.4 DISASTER RECOVERY PLAN UPDATES AND DISTRIBUTION **69**
5. APPENDIX *69*
Facilities Emergency Procedures **69**
Master Employee Listing **69**
Damage Assessment Checklist **69**

Directions to Emergency Operations Centers 69
Approved Press Release 69
6.2 GIT Financial Statements 73

1.0 SECTION ONE: INTRODUCTION AND EXECUTIVE SUMMARY

1.1 Background

The Nigerian Stock Exchange (NSE) was established in 1960 and currently has over 280 listed companies with a total market capitalization as at the end of 2005 of approximately $20 billion. All listings are included in the only index, the Nigerian Stock Exchange All Shares Index. The Nigerian Stock Exchange and its management team understand the importance of a reliable stock exchange and have requested the U.S. Trade and Development Agency (USTDA) "Technical Assistance" to facilitate development of a disaster recovery plan (DRP).

The DRP will provide a mechanism for continuous trading and support of the NSE in case of failure of the main building or main equipment and ensure that the data stored and transferred on the NSE's hardware and communications infrastructure is fully recoverable and secure.

The Technical Assistance will include the review of existing IT systems and plans, existing hardware and communications infrastructure, and would develop a strategic plan, specifications, and an implementation plan for a disaster recovery facility. The Technical Assistance will also ensure that any recommended procurements can be integrated with existing hardware, communications infrastructure, applications, and databases.

GIT is very pleased to present this comprehensive proposal to be selected as the consultant to provide Technical Assistance as specified for NSE.

1.2 Work to Be Accomplished

To accomplish the Technical Assistance for NSE, GIT will:

- Review of existing IT systems and plans, existing hardware and communications infrastructure, and
- Develop a strategic plan, specifications, and an implementation plan for a disaster recovery facility.
- Ensure that any recommended procurements can be integrated with existing hardware, communications infrastructure, applications, and databases.

The primary scope of the work to be performed under this proposal is to:

- Produce the DRP Report for the NSE environments
- Define the time criteria for restoring the NSE's operating environment
- Document the provisions for recovery of mission critical IT processing capabilities and Applications within the time frames provided by the plan.

This project does not include funds to:

- Purchase any software tools or packages that may be recommended as a result of work on this project.
- Perform tests of the effectiveness of the disaster recovery procedures documented in the plan
- Conduct or support any new/modified Vendor Agreements
- Negotiate or support any new/modified internal Agreements
- Perform training on any selected and implemented tools.

GIT will work directly with the NSE liaison to complete this project in seven (7) broad Stages that comprise approximately forty (40) key Tasks.

GIT will utilize a set of proprietary templates that will be customized for use by NSE. These templates will enable the critical DRP information to be gathered and documented quickly and efficiently. The data gathered will then be supplemented and ratified through selected interviews with key personnel.

In aggregate, the data gathered will form the basis for comparison to industry-based Disaster Recovery Planning Best Practices. The resulting Gap Analysis will be documented as a critical component of the "NSE DR As-Is Assessment" delivered to NSE.

GIT will utilize the Gap Analysis and DR Assessment along with the DR Best Practices and its extensive experience to develop and document the critical procedures, forms and reports that will be integrated into an overall NSE DR Facility Development Plan.

1.3 DRP Stages & Tasks

Over the course of the project specifically, GIT will:

1. Complete DR Data Gathering & Current State Assessment
2. Document Emergency Response Procedures
3. Document Plan Activation Procedures
4. Document Administrative Procedures
5. Document Key DR Reports
6. Document Key DR Forms
7. Final Delivery & Reporting

In each Stage of the NSE DRP Project, GIT will complete one or more key Tasks.

DR Data Gathering & Current State Assessment

GIT will complete this stage of the project in three tasks:

- Identify key Areas/individuals
- Distribute/Conduct Data Gathering Template(s)
- Complete Gap Analysis & DR Assessment

Document DR Emergency Response Procedures

Emergency response ensures that all parties act to quickly determine the emergency and take appropriate action. GIT will complete this stage of the project in three tasks:

- Emergency Evacuation Procedures
- Emergency Phone Numbers
- Emergency Notification Procedures

Document DR Plan Activation Procedures

Plan activation ensures that all parties and all materials are coordinated for the DR Facility. GIT will complete this stage of the project in ten (10) tasks:

- Activate Incident Management Team
- Activate Emergency Operations Center
- Emergency Declaration Procedures
- Relocate Operations Procedures

- Situation & Damage Assessment Procedures
- Communications
- Offsite Storage
- Purchasing procedures
- Recovery Site Generator, Electrical & Security plan Procedures
- Reconstruction Procedures

Document Administrative Procedures

The administrative responsibilities summarize NSE policy. These responsibilities and procedural guidelines must be applied throughout the initial response and any subsequent business recovery activities.

- Enforce NSE Policies
- Monitor & Report Recovery process
- Maintain Recovery Related Record Keeping
- Define Testing & Maintenance Functions

Document Key DR Reports

The Reports are a critical mechanism for communication throughout and after the Disaster/Recovery period.

- Business Unit Key Contacts
- Summary of Critical Applications, Servers & Recovery Time Objectives (RTOs)
- Vendors & Suppliers
- Summary of Desktop & Workspace Requirements
- Other Equipment
- Critical Telephone Numbers Report

Document Key DR Forms

The Forms are a critical support provided to all Recovery Teams for use throughout and after the Disaster/Recovery period.

- Recovery Activities Log
- Critical Files & In-Progress Assessment
- Critical Equipment & Assessment
- Personnel Locations Control Form
- Time Sheet tracking
- Telephone Log
- Damage Control Status
- Bomb Threat Response
- Injury Status Reporting
- Receiving Room Sign-In

Final Delivery & Reporting

The final requirements and procedures for the DR Facility will be documented and delivered in this Stage. The DR Implementation Plan and Final Report are key to completing the project.

- Develop DR Implementation Plan
- Document & Deliver Final DR Report
- Conduct Final DR Presentation

1.4 DRP Deliverables

In completing this important project for NSE, GIT will produce over 30 discrete Deliverables. The table below shows the schedule of Deliverables developed by GIT by stage of the project.

	Stage	Deliverable(s)	Schedule
1	DR Data Gathering & Current State Assessment	• NSE Current State DR Assessment	Sept 2006
2	Document DR Emergency Response Procedures	• Emergency Evacuation Procedures • Emergency Phone Numbers • Emergency Notification Procedures	
3	Document DR Plan Activation Procedures	• Activate Incident Management Team • Activate Emergency operations Center • Emergency Declaration Procedures • Relocate Operations Procedures • Situation & Damage Assessment Procedures • Communications • Offsite Storage • Purchasing procedures • Recovery Site Generator, Electrical & Security plan procedures • Reconstruction Procedures	Sept / Oct 2006
4	Document DR Administrative Procedures	• Enforce Company Policies • Monitor & Report Recovery process • Maintain Recovery Related Record Keeping	Sept / Oct 2006
5	Document DR Reports	• Business Unit Key Contacts • Summary of Critical Applications, Servers & RTO's • Vendors & Suppliers • Summary of Desktop & Workspace Requirements • Other Equipment • Critical Telephone Numbers Report	Nov / Dec 2006
6	Document DR Forms.	• Recovery Activities Log • Critical Files & In-Progress Assessment • Critical Equipment & Assessment • Personnel Locations Control Form • Time Sheet tracking • Telephone Log • Damage Control Status • Bomb Threat Response • Injury Status Reporting • Receiving Room Sign-In	Nov / Dec 2006
7	**Final Delivery & Reporting**	• **DR Implementation Plan** • **Final DR Report Master** • **Final DR Presentation**	**Dec 2006**

1.5 The GIT Team

GIT expects Stage I to start on or about 11 September 2006 and be completed on or about 29 December 2006.

In order to accomplish this, GIT has assembled a seasoned world-class team of professionals with the experience, skills and pragmatic knowledge necessary to complete this important project.

GIT is a US business firm that has extensive International experience.

GIT has successfully worked in and implemented large, technically complex projects in a variety of commercial and governmental environments.

GIT has extensive BCP experience and a long track record of successful delivery.

GIT looks forward to working with NSE to successfully accomplish this critical project for the people of Nigeria.

2.0 SECTION 2: COMPANY INFORMATION

2.1 Company Profile

Global Information Technology, Inc. (here in after referred as GIT or Contractor or Offeror) is a U.S. based firm that has become a leading provider of information technology services to large and medium-sized organizations world-wide. GIT is focused on providing its clients with the most efficient and cost-effective solutions while maintaining the highest levels of quality. (Note: See Appendix 6.2 for attached GIT Financial Statements).

GIT opened its office in the US in 1995. GIT has grown to approximately 85 employees including 70 full time & 15 Sub-contractors, with 4 regional offices in the US in the last 11 years. GIT also maintains office space & employs over 300 software engineers in India & over 50 software engineers throughout Europe. GIT now provides information technology services in more than 6 countries from the following offices:

Tampa, FL	Dallas, TX	Indianapolis, IN
Raleigh, NC	London, UK	
Hyderabad, India		

As an accomplished provider of technology services, GIT has grown into a leader in the full service information technology outsourcing industry. GIT has successfully delivered large-scale external outsourcing services especially on IBM mainframe to MCI, Caterpillar, Lincoln National Life Insurance Corporation, Eckerds, IBM, FCCI, BellSouth, Lucent Technologies, EDS, UPS, Fidelity Investments, Beech Street Corp., and other large corporations.

1. GIT Headquarters is located at 8913 Regents Park Dr. Suite # 680, Tampa, FL-33647 PH; 813-973-1061, Fax: 813-973-4370 web-address: http://www.git-org.com

2. Year Established: 1995 in USA

3. Type of Ownership: A Florida Corporation

4. Project Manager's Name and Address: Irv Brownstein, Address: Same as Above.

GIT's methodologies and procedures have been tested within the information technology industry with excellent results.

MISSION STATEMENT:

To build and sustain long-term relationships with all our clients by providing critical, high quality & cost effective solutions, using the best human resources available through the application & integration of existing and emerging technologies with the aim of maximizing growth opportunities for our clients, employees and associates.

2.2 Company Philosophy

In meeting its corporate objective of quality services, GIT adheres to the following fundamental principals:

CUSTOMERS AS PARTNERS:

GIT strives to build "lifetime" relationships with its customers by providing them with the highest quality services, advanced technology, and added value in order to earn and maintain their respect, trust, and loyalty. We recognize that true partnership must be based on an interactive working relationship. Our contribution to this relationship is our expertise in solving our customer's business problems, in addition to our interminable commitment to excellence. The services we provide are based on professional competence, integrity and openness.

OUR PEOPLE:

We place a very high value on the loyalty, dedication and creativity that our employees bring to GIT. A critical success factor has been our ability to secure, train and retain high-quality people. Our personalized career and education programs keep our employees current in their areas of expertise and informed of the direction of the industry.

GIT's professionals are among the best in our industry and we are confident in their ability to meet or exceed the expectations of our customers.

INTEGRITY:

GIT adheres to a strict code of business conduct that ensures that our employees maintain the highest standards of business ethics in all dealings with customers, suppliers, fellow employees, and the general public.

QUALITY:

GIT continuously strives for excellence by providing high-quality, high-value deliverables to its customers. By achieving this goal, we ensure that our customers are proud of the work we have delivered for years to come and that they regard GIT as their technology partner of choice. GIT enhances the value of services provided by using highly respected software development/enhancement methodology as well as quality management and assurance programs. These methodologies and programs are customized for our customers to most effectively introduce and reinforce the principles and procedures for achieving total quality. GIT clearly demonstrates an unyielding commitment to customer service and quality in the delivery of a consistently superior work product.

Our ultimate goal **Total Customer Satisfaction.** In order to accomplish this goal, we must gain a thorough understanding of our customer's business and technical strategies and then deliver the best possible solution utilizing our advanced technology, proven methodologies and solid base of experience and expertise.

2.2 Offeror's Authorized Negotiator

Suren K Ajjarapu, Executive President
Global Information Technology Inc.
8913 Regents Park Drive
Suite #680
Tampa, FL 33647
Tel: 813-973-1061 Ext. 226
Fax: 813-973-4370

2.3 Negotiation Prerequisites

1. No impact of current commitments.

2. None.

Authorization and Approval

1. RESPONSIBILITIES OF THE PARTIES

NSE:

NSE is responsible to identify the key individuals, SMEs and any related Vendor personnel that GIT will interview and ensure that they make themselves reasonably available for interview, review and discussion sessions that will typically not exceed ninety (90) minutes in duration.

NSE will provide timely access to and/or working copies of the most current data, charts, reports, templates and other contents related to NSE and as described in the Template (See Appendix 6.1).

NSE will provide timely response to all requests for information related to NSE and as described in the Template (See Appendix 6.1).

NSE agrees to make best efforts to coordinate each topic session so that they can be accomplished in one (1) or two (2) visits to the NSE's locations or by phone.

NSE is also responsible to provide an environment (a meeting room or other facility) for these interviews that is conducive to effective completion of the work with minimal distractions.

GIT:

GIT will assign Irv Brownstein as the Project Manager.

This consultant will conduct the interviews, provide the Final DR Report, conduct the Final DR Presentation and answer NSE's questions for the duration of this project.

This consultant will work with NSE on all matters related to this project.

GIT will make best efforts to complete all work prior to year-end 2006.

2. DURATION OF WORK

The elapsed time required to perform the Service begins on NSE Authorization.

The work will be considered complete with the delivery of the Final DR Report.

GIT is not responsible for delays in the process caused by NSE in the scheduling of interview, work and data gathering sessions.

3. PAYMENT

GIT will invoice NSE for the Services as defined below.

	Stage	Percent Due	$$
I	Upon Project Approval & Execution of Contract	**20%**	$47,282
II	Upon Delivery of Section 4: Stages I & II	**40%**	$94,564

	Stage	Percent Due	$$
III	Upon Delivery of Section 4: Stages III & IV	20%	$47,282
IV	Upon Delivery of Completed Report & Presentation	20%	$47,282
Project Totals			**$236,410**

NSE agrees to pay each invoice in full within thirty (30) days after the date of the invoice.

LIMITATION OF LIABILITY

The cumulative liability of the GIT to NSE for all claims relating to the service, in contract, tort, or otherwise, shall not exceed the total amount of all fees paid by NSE to the GIT for the service during the immediately preceding six (6) months.

In no event shall GIT be liable to NSE for any consequential, indirect, special, or incidental damages, even if GIT and NSE have been advised of the possibility of such potential loss or damage.

The foregoing limitation of liability and exclusion of certain damages shall apply regardless of the success or effectiveness of other remedies.

NO WARRANTY

The parties agree that GIT makes, and NSE receives, no warranties, express, implied, statutory, or otherwise. The service is provided "as is."

The GIT specifically disclaims any warranty of merchantability or fitness for a particular purpose.

AUTHORIZED MANAGEMENT SIGNATURE:

GIT, INC.

By: _____

Name: _____

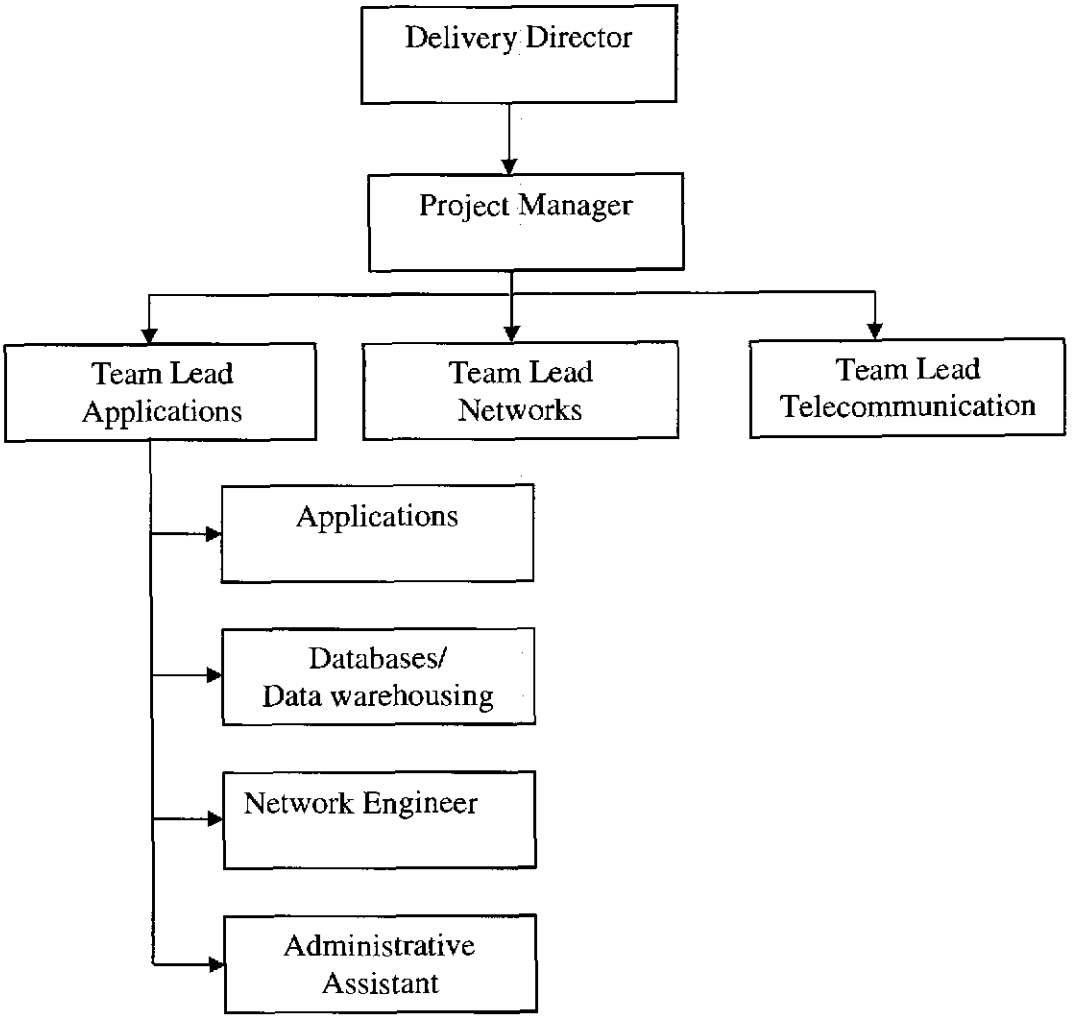
Title: _____

Date: _____

3.0 SECTION 3: ORGANIZATIONAL STRUCTURE, MANAGEMENT, AND KEY PERSONNEL

3.1 Organizational Structure

GIT Management Organization chart



3.2 Delivery Management Team

GIT Delivery Director

Mike Ike

SUMMARY

Mike brings over 20 years of professional business experience to the table. He has held numerous leadership roles in Information Technology, Program/Project management, Organizational Change Management, Business Process Management, System Implementation and Integration, Team Building,

Software Testing, Operations management, Disaster Recovery and Business continuity Planning, IT Strategy and Execution, Enterprise IT Optimization and Vendor Management and Contract Negotiations.

Mike has a track record in ensuring Information Technology is consistent with business strategic and operational needs. He effectively manages customer expectations and ensures appropriate Change Control processes. All of these leadership skills consistently deliver IT projects that are well staffed with the right talent, exceed customer expectations and are completed on time and on budget.

INDUSTRY EXPERIENCE

- Telecommunication, Information Technology, Transportation, Insurance, Government and Education

PROFESSIONAL EXPERIENCE

Chief Technology Officer, City of Memphis, TN (2004 – Present)

- Provides guidance and counsel to the executive team in the examination and definition of objectives for existing and/or proposed information systems and the design of improved systems
- Manages the implementation of Oracle E-Business Suite 11.5.9: Financials, CRM, DBI and HRMS/Payroll, a 16M Project, renegotiated contract with Oracle and saved City of Memphis $2.5M
- Manages the upgrade of Oracle E-Business Suite from 11.5.9 to 11.5.10
- Consistently interfaces with all the 22 City Divisions to identify opportunities to standardize technical solutions and realize synergies in technology across the entire enterprise
- Manages implementation of City-wide imaging scanning solutions (content management)
- Leads the planning and development of City-wide strategies for generating resources and revenues for information technology
- Leads, guides, and oversees the City of Memphis information technology the process of determining the priorities, projects, and future directions of the budgeting process, and provides leadership in cost and productivity analysis
- Provides City-wide leadership and direction in the management and operation of information technologies and services across the City
- Manages the development and implementation of disaster recovery and business continuity plan for the City of Memphis
- Manages implementation of City-wide security system and Fuel management system
- Manages the development and implementation of proprietary Revenue System

- Leads and coordinates the development and implementation of integrated, strategic IT plans and policies for the City of Memphis

- Developed five year City of Memphis Information Technology Strategic Business Plan

Executive Vice President /Chief Technology Officer, iMcG, Atlanta, GA (2002 – 2004)

- Responsible for driving the full consulting life cycle for the Eastern region and regional growth by working with strategic partners to identify marketplace trends and their implications for new business/solution development
- Responsible for critical client interface to understand their business objective, goals and challenges and leveraged benchmarking to identify "best practices" and drive implementation of "best of breed" technology solutions.
- Managed high level post implementation reviews of (ERP) PeopleSoft Payroll application suites for both Bellsouth and UPS
- Leaded cross-functional teams in defining requirements, developing project plans, acquiring resources, and implementing solutions
- Utilized iMcG BPM Methodology and Tools to drive small & complex projects

- Developed and implemented iMcG BCP HealthCheck methodology to review the current disaster recovery capabilities of data processing, telecommunications and networks
- Participated in performance management process and demonstrated integrity, respect, commitment to excellence, collaboration, agility and valued diversity
- Conducted business impact analyses and assist company units to determine critical business process, identifies acceptable recovery level and time periods, and establishes resources required for the successful resumption of business operations in the event of a disaster
- Developed organizational transformation methodology and tools for iMcG business offerings
- Developed and implemented Integrated Services for iMcG go to market products
- Responsible for corporate financial planning, analysis and P&L statements

Principal Consultant/Sr. Project Manager, FedEx, Memphis, TN (1997 - 2003)
Software Engineering Services Project

- Managed the migration of Revenue Systems from Mainframe platform to Chronos (Client Server) platform, a $750M project
- Lead the business plan development effort, assessing performance against plan targets, and make changes as needed to improve performance
- Responsible for management of the financial reporting, billing, collections, revenue recognition, flexibility, controls, stability and capacity, customer benefits
- Worked with FedEx Management team and Business Development to help determine the timing of bringing in new projects based on new business requirements and funding availability
- Development of consulting related tools/templates; proposal templates, estimating
  Tools integrated with FedEx implementation methodology templates
- Administered project staffing, conflict resolution processes, and resource utilization
- Managed Full Cycle test, test execution and test verification
- Managed a very large scale integration test, test execution and test verification
- Managed a System test, test execution and test verification
- Responsible in recruiting top talents, training/deploying/coaching/mentoring
- Prepared project progress report for the Management team

Proven Ground Project

- Managed project management office, a $20M Project with a team of 45
- Participated in strategic planning for Express Load
- Implemented and managed Primavera and Webster Time reporting tool
- Prepared monthly progress report for the Management team
- Managed implementation of multiple systems
- Managed online processing for Worldwide revenue application
- Managed the development and implementation of disaster recovery and business continuity plan for FedEx
- Participated in product negotiations and vendor selections
- Managed customer expectations and deliver quality service on time and under budget as well as managing an on-going relationship with customer

Y2K Project

- Managed the development, implementation and documentation of Y2K renovation strategy
- Provided strategic recommendations and contingency plans required for FedEx to implement Y2k project
- Managed 175 computer professionals includes DBA, project leaders, System and application programmers, a $150M project
- Reported directly to the VP of information systems
- Chaired five different meetings: year 2000 testing meeting, year 2000 systems software meeting, year 2000 application meetings, year 2000 integration meeting and year 2000 client server meeting
- Prepared meeting minutes and monthly progress report for the Management team

- Managed the implementation of (ERP) PeopleSoft Payroll application suites
- Managed the design and implementation of separate MVS platform dedicated for Y2K project
- Managed the implementation of HourGlass 2000 for Y2K testing
- Managed Y2K test, test execution, test verification and test certification
- Ensured that systems, software and applications are year 2000 compliant
- Participated in product negotiations and vendor selections

Sr. Project Manager, IBM/Lucent, Atlanta, GA (1996- 1997), Telecommunication Out-Sourcing Engagement

- Directed the migration activities of all-Lucent Technology Payroll application from AT&T a $2B Out-Sourcing engagement.
- Managed the integration of Lucent Technology payroll system to a new payroll system
- Developed migration strategy and continuous maintenance support strategy of data centers.
- Managed the vendor selection process for contractors
- Managed overall day-to-day operation of 3 data centers
- Hired and indirectly managed teams of 150 with direct report of 10 managers from development, enhancement, testing and production support.
- Managed a $55m budget
- Integrated all Lucent Technology data centers from 35 to 3 data centers reducing annual cost by $15M

Sr. Project Manager, IBM/GTE, Tampa, FL (1994 – 1996), Telecommunication Out-Sourcing Engagement

- Managed a Telecommunication Billing Application Out-Sourcing project for GTE.
- Developed migration strategy from GTE data center in Thousand Oaks California to Tampa Florida
- Developed migration strategy from GTE data center from Tampa Florida to Fort Wayne Indiana
- Conducted research on good practices for managing and running a successful Out-Sourcing project.
- Managed a team of Developers, Enhancement, Testing and Production support
- Managed Client/Vendor relationship, Researched and implemented best practices

State Farm Insurance, Winter Haven, FL (1988 –1994)
Systems Controller II

- Managed the development and implementation of Healthcare application for State Farm Insurance
- Managed the implementation of production automated scheduling systems and trained the employees
- Responsible for budgeting, salary administration, policy administration, performance planning and review
- Involved in the interviewing and hiring process, making sure that associates have the right skill set
- Maintained contact with customers, engineers, development groups and users in the event of hardware or software problems
- Coordinated various projects, planning, implementation and scheduling of new projects
- Responsible for day to day IT operations to ensure that we met our deliverable

Systems Analyst

- Performed detailed analysis and prepared documentation for resolutions of production and technical problems
- Provided operational DB2 / IMS application support, system and sub-system monitoring, batch processing, performed system measurement analysis, system recovery, problem analysis resolution
- Modified JCL / PROC, performed MVS / JES2 upgrades, systems tunings, IMS upgrades, database migrations, database conversions, and libraries upgrades, coordinated disaster recovery
- Performed change / problem management and coordinated changes, ensured that known problems were corrected in a timely manner and associated changes were coordinated across the company

Management Trainee

- Received intensive training with development group, MVS / IMS technical support, operation support, worked on several projects and made several presentations to senior managers, performed practice management
- Responsible for network scheduling and auto flow changes to increase efficiency, modification of JCL / PROC, coded program and JCL, performed abend analysis, monitored batch processing in Test and Production environments
- Troubleshoot hardware and software problems, worked with users to identify their problems and resolve them, monitored system by utilizing IMS, MVS / JES2 and VTAM commands, used IBM utilities and IDCAMs to manipulate datasets and VSAM respectively
- Performed system measurement analysis, database conversions, database migration, MVS/JES2/IMS upgrades and write test case per business requirements

Other Professional Experience, Daytona Beach, FL (1986 – 1988)

Assistant Professor (Bethune-Cookman College)

- Instructed undergraduate level courses on principle of supervision, qualitative analysis and business policy

Career Counselor

- Counseled students on career planning and development, organized and facilitated employability skills seminars, conducted career exploration sessions for all students, administered and interpreted career interest inventories for all students, monitored and maintained career resources center for students and faculty members

Application Developer Lead (Embry-Riddle Aeronautical University)

- Managed and implemented the inventory application for the entire university system

EDUCATION

- MBA, Embry-Riddle Aeronautical University, Daytona Beach, Florida
- BS, Business Administration, Bethune-Cookman College, Daytona Beach, Florida

GIT Project Manager

Irv Brownstein

SUMMARY

A consultant with over thirty years experience in the information industry. In the course of his career he has demonstrated particular expertise in the areas of metrics, balanced scorecards and measurement programs, business intelligence, program management, business continuity & disaster recovery, software asset management, process engineering, skills management, all phases of systems development and implementation, software package evaluation and installation, systems methodology development and implementation, productivity improvement and cost reduction, quality assurance and project management.

He has designed, developed and implemented a variety of IT effectiveness, re-engineering, skills management and measurement programs in both the public and private sector. He has developed and marketed software packages and authored How To Select the Right Software (ECP).

ACCOMPLISHMENTS

CITY OF MEMPHIS (2006) Developed an IT Strategic Business Plan for the City of Memphis. The Strategic plan centered around a functionality and training implementation assessment for Oracle Financial, Budgeting, Purchasing, HR/Payroll, CRM & Balanced Scorecard. Lessons Learned were

incorporated into next phase plans for Oracle module upgrades, training plans and implementation of new EAM and Sourcing modules. The Oracle Functional component was then incorporated with a series of IT Technical & Support Strategies that addressed Communications Strategy, Geographical Information Systems (GIS), Web-based Programs, Hardware, Software & Procedural Standardization Programs, Asset Management, and Security. An overall ROI was developed along with a Risk based analysis of the challenges to success.

CITY OF MEMPHIS (2006) Developed a Business Continuity Planning & Disaster Recovery plan for the City of Memphis. The IT Disaster Recovery Plan addressed the Oracle based systems environment (AP/GL/AR/Budgeting, HRMS, and OAB) ERP, with other distributed, client server and web-based software applications; defined the time criteria for restoring the City's operating environment; documented the criteria, materials, policies, procedures, forms and reports for recovery of mission critical IT processing capabilities and Applications within the time frames provided by the plan.

AMERICAN ELECTRIC POWER (2006) Conducted a process assessment and gap analysis of the Quality Assurance (QA) Testing & Change Control function in Columbus, Ohio to identify opportunities for improved effectiveness. Focus of the effort included review of QA tools, practices, procedures, testing approaches and environments as well as the SDLC, Requirements Management, Measurement & Analysis, Document Change Control. Responsibilities included: Documenting the current state (Findings & Observations); Defining a "To-Be" state and Recommendations based on "Good Software Engineering Practices"; Developing a gap analysis, and Defining a Game Plan improvement plan to close the gaps.

CITY OF MEMPHIS (2005) Developed and implemented a Balanced Scorecard based performance measurement and management program for the City of Memphis. Functional responsibilities encompassed identifying, designing and documenting 544 performance measures/KPIs for 20 city divisions and agencies (Fire, Police, Public Works, etc.) and developing a phased implementation plan. Technical responsibilities included system set-up, measure and KPI design and building over 100 balanced scorecards in 3 levels with custom views to support the overall City-Wide objectives. Requirements were gathered through a custom questionnaire (118 completed), 51 work sessions involving 334 of the top city managers yielding over 1300 pages of requirements. The custom KPIs, supporting processes, data sources and related initiatives were documented, integrated and implemented using Oracle Balanced Scorecard (BSC 5.1) and Oracle Daily Business Intelligence (DBI 7.1). The project integrated data from Oracle modules, 29 Non-Oracle systems and conversion of existing reports.

VERISIGN (2005) Conducted an assessment of the Quality Assurance (QA) and Testing function to identify opportunities for improved automation and reduced elapsed time. Responsibilities included review of approaches, tools, practices and procedures for the QA testing area in order to understand the current state of automation, analyze key report testing practices and complexities, and develop a set of recommended improvement actions to take.

ONEBEACON (2005) Conducted a process assessment and gap analysis of the Quality Assurance (QA) and Testing function to identify opportunities for improved effectiveness and reduced elapsed time. Responsibilities included review of approaches, tools, practices and procedures for the business, development and QA areas in order to document the current state, develop a gap analysis, and define a Roadmap improvement plan to close the gaps. This assessment was conducted at facilities in Foxboro, MA and Philadelphia, PA.

CYBERTHINK (2005) Developed a Business Continuity Planning & Disaster Recovery plan for this major consulting company and development center. The IT Disaster Recovery Plan addressed the current systems development, testing, production and client managed systems environments with other distributed, client server and web-based software applications; defined the time criteria for restoring the operating environment; documented the criteria, materials, policies, procedures, forms and reports for

recovery of mission critical IT processing capabilities and Applications within the time frames provided by the plan.

AMERICAN RED CROSS (2004) Conducted a process assessment and gap analysis of the Information Technology function relative to designated standards and industry best practices. Responsibilities included review of IT practices and procedures for both regulated and non-regulated segments of the business, determining and documenting the current as-is state within IT, defining the future to-be processes based on CMMI and ITIL, developing a gap analysis between the As-Is state and the To-Be state, and develop a Roadmap improvement plan to close the gap.

ASSESSMENT MANAGER METHODOLOGY (2004-2005) With ECP developed an independent proprietary assessment methodology supported by a series of workshops and tools for determining an organization's software maturity and capabilities. The assessment methodology provides comparative analysis against a defined maturity model and database of baseline values in order to focus impact of change on savings, compliance and risk reduction through process improvement. In addition to training workshops the service provides an array of planning, assessment and reporting tools.

PERFORMANCE MEASUREMENT PROGRAM (2003) For the Workplace Financial Services (WFS) area of JPMORGAN CHASE, designed, developed and implemented a measurement program to support the department's performance tracking and process improvement program. Working with the management team and process improvement teams gathered custom requirements, developed and gained approval of an overall Metrics Strategy and integrated Project Plan for a series for a series of tactical program releases. Designed, documented and implemented initial release measures through a Balanced Score Card (BSC) reports. To support implementation conducted staff metrics training, documented a comprehensive Metrics Reference Guidebook and established a BSC Change Management program.

ITIL BENCHMARK PROGRAM (2004-2005) With ECP developed an independent ITIL Readiness Assessment methodology, ITIL Metrics and database for establishing ITIL ROI. The benchmark program establishes and maintains a proprietary database that identifies the key planning factors and savings potential related to an organization's ITIL maturity. The program provides the baseline and ROI impetus from which to launch or improve an ITIL program and allow an organization to track its benefits. The program includes training, a centralized database to track ITIL benefits and benchmarks; published reports of trends and findings; ITIL Maturity Model; data collection tools to gather savings and other ROI factors by ITIL component. Program materials, including updates, are included in the ITIL Benchmark Handbook.

PERFORMANCE MEASUREMENT PROGRAM (2002 - 2003) For ALLSTATE (IT area of 2000 developers) designed and developed the measurement program to support CMM software process initiatives to reach Level 3, implement department software process performance improvements and integrate with the organization's balanced scorecard. Developed and gained approval of an overall Metrics Strategy and integrated Project Plan for a series for a series of tactical program releases. Designed, documented and implemented initial release measures through a series of production Dashboard Reports. To support implementation, developed and conducted staff metrics training, documented a comprehensive Metrics Reference Guidebook and established a Metrics Repository.

PROJECT MANAGEMENT SOLUTIONS GUIDE (2002) For Isogon Corporation worked with the management team to identify, determine and document each of the products, services, training seminars and business partners available to build a customer specific solution. The solutions guide also included a high-level implementation plan as a template in MS Project that encompasses all of the potential work steps as well as the associated estimated effort and roles needed for successful implementation.

METRICS PROCESS REENGINEERING (2002) For UNITED HEALTH CARE evaluated current operational balanced scorecard, metrics calculations, data sources, procedures, and processes. Formulated

management proposals to streamline time to deliver, staff support needed and long term automation. Implemented re-engineered solutions for the organizations metrics reporting process and repository. Developed a metrics guidebook to document measures with detailed operational procedures.

AUDIT PROJECT AND COMMUNICATION MANAGEMENT (2000-2001) For PRUDENTIAL insurance company, representing a 300-person highly regulated nation-wide project:

- Managed the audit effort for the project as the primary point of contact with all external groups.
- Established and supported knowledge management system (3500 documents) in Lotus' Domino.doc.
- Produced key project documentation products including: 80 page project architecture overview; 100 page project reporting / operational controls guide; 300 page Call Center Training Facilitator Guide.
- Developed the project's documentation standards, templates and Business Continuation Plan.
- Managed all external project reporting (10): status, production, financial.

BUSINESS CONTINUITY/DISASTER RECOVERY PLAN (1999) For PRUDENTIAL insurance company, established the planning unit for a 500 person $45 million systems and operations organization. Established, coordinated and completed the department's Records Management Program and Business Continuation Plan. The IT Disaster Recovery Plan addressed the current systems development, testing, production systems environments with client server and web-based software applications; defined the time criteria for restoring the operating environment; documented the criteria, materials, policies, procedures, forms and reports for recovery of mission critical IT processing capabilities and Applications within the time frames provided by the plan. Also developed a comprehensive Record Management System.

KEY PERFORMANCE MEASURES & PROCESS IMPROVEMENT (1998-1999) For EBS DEALING SERVICES, INC. established and maintained an array of Key Performance Measures (KPM) for the Technology and Operations department. Results and trends were summarized monthly in a report to senior management. Projects included: Time Sheet Effort Analysis, Earned Value Point approach, SDLC Project Control Checklist (all phases and deliverables of life cycle), Product Development life-cycle, as well as Project and Problem Management Process charts. Focus of the organization was to achieve CMM Level 2. Conducted training presentations on CMM and KPAs for staff (over 100). Key performance measures, scorecards and SDLC templates were used.

TECHNICAL PLANNING (1997-1998) For PRUDENTIAL insurance company, established the planning unit for a 500 person $45 million systems and operations organization. For the department executive, developed the organization charter, defined a broad array of functions and defined team job definitions. Formulated scenarios and management approaches to save over $5 million (in 3 months) for budget alignment. Assisted the management team in planning, budgeting, communicating and completing projects. Established, coordinated and completed the department's Business Systems Plan, Budget. Developed, implemented and supported corporate and business systems measurement efforts. Developed and supported Systems Development Life Cycle and SEI/CMM assessments, goals and reporting on a department-wide basis. Focus was to achieve CMM Level 2. Conducted training presentations on CMM and KPAs for staff (over 150); developed customized review checklists; conducted internal assessment by KPM for department head.

SKILLS MANAGEMENT (1997-2001) For RELIANCE INSURANCE, UNITED AIRLINE, PERSHING and PUBLIC SERVICE ELECTRIC & GAS COMPANY (NJ), completed skills assessment/management programs. For each company determined current skills across technical and business functions; developed gap analyses of skills to standards and projected needs; developed data collection and reporting processes, developed training curricula for improvement; developed new skill based job families to consolidate existing titles; and, preparation of position descriptions.

APPLICATION & LOAN ADMINISTRATION PROCESS For the consumer asset area of a large NY based bank, completed a project to re-engineer existing workflow and implement a comprehensive

performance measurement program. The project produced an operational instrument panel for ongoing management of productivity, quality and portfolio indicators against a baseline assessment of the current and revised delivery process.

MANUFACTURING MEASUREMENT PROGRAM Implemented a measurement program and Information Systems Assessment for a large premium tire company. Responsibilities included facilitating workshops to gather productivity requirements and management practices; developing and scoring data collection surveys; defining productivity metrics; determining the company's 3 level Dashboard Reports; developing a comprehensive metrics guidebook to document the measurement program.

PRODUCTION AUDIT PROCESS Conducted Operations Reviews and "Friendly" audits for a medium size insurance company and several areas of the largest bank. These efforts focused on a comprehensive review, evaluation and action plans regarding the existing facilities, workflow, procedures, security, backup and disaster recovery plans.

CLIENT/SERVER PROJECT ESTIMATION For a large investment bank, reviewed and modified process for estimating client/server projects. Existing planning process was reviewed and revised. Through a new series of business questions and a new client/server project "life cycle." Was able to calibrate the CA-Estimacs product to generate estimates within 10% of actual effort and cost.

STRATEGIC TEST PLAN Strategic Test Plan and management Programs for implementation of a comprehensive administrative system for a large insurance/financial services firm. Defined test strategies and objectives, test approaches and standards, project plans, user acceptance product test plans, testing summary reports, change control and problem reporting programs, training plans and contingency plans.

BUSINESS RE-ENGINEERING Participated in the complete process re-engineering of the Corporate Trust Business are for a large New York bank. Responsibilities included workflow analysis and redesign, determination of personnel savings, identification of automation opportunities and definition of the resulting overall workflow and application architecture.

CHECK PROCESSING PERFORMANCE MEASUREMENT Developed a Measurement Program and conducted a process and productivity Assessment related to the measurement program for the Check processing area of a large NY based bank. The opportunity assessment identified process improvement savings in excess of 25% of the area's budget.

APPLICATION SUPPORT PRODUCTIVITY Conducted an Application Support Productivity Review for a large insurance/financial services firm's entire maintenance portfolio. The project focused on the client's desire to improve process efficiency and the productivity of application support.

PROCESS IMPROVEMENT For the largest back-office brokerage company, evaluated and revised the existing development process built around a customized version of a premier enterprise methodology in an MS Project Template that addressed all QA and Project Management activities and was implemented for a development staff of over 300.

FINANCIAL SERVICES PERFORMANCE MEASUREMENT Implemented a comprehensive measurement program, quality assessment, process and procedure assessment leading to re-engineering all internal processes as the basis for extensive productivity improvements for the 800-person systems organization in both Florida and Phoenix for this Phoenix, AZ based charge-card conglomerate.

MUTUAL FUND MEASUREMENT PROGRAM Implemented a Measurement Program and Information Systems Assessment for a major mutual fund group. This effort focused on the client's desire to improve productivity and quality for both new development and application support. Responsibilities included gather productivity requirements; management practices; defining productivity

metrics; determining the company's baseline for Technical, Functional and Process Quality; establishing an ongoing measurement program; and, preparing an overall assessment of the IT function.

SYSTEMS DEVELOPMENT METHODOLOGIES Prepared Customized Systems Development Methodologies for the largest insurance company, a motion picture corporation, large chemicals corporation, large cable network, major communications firm, the largest credit rating service and a large Chicago based bank. Evaluated, selected and installed vendor methodologies for several companies.

SOFTWARE TOOL SELECTION Developed Software Tool Evaluation and Selection Guidelines for a major government agency for use throughout the federal government. This book focused directly on software tools to establish a software engineering technology. The book was supported by a two-day training workshop developed and conducted for personnel from several government agencies.

HARDWARE: IBM 370/168, 3032, 3083, 3081, 3090, 43xx; AS/400; DEC PDP 11/70; UNIVAC 9200; HP/3000; MSI; Apple, Intel based.

METHODOLOGIES: Project Workbench and Modeler, Microsoft Project; SPECTRUM International; Method/1; Gane and Sarson; Warnier/Orr, De Marco: Yourdon; firstCase; SLIM; CA-Estimacs/PlanMacs; CA-Metrics; CorManage (Scorecards); Rapid Scorecard; FPWorkbench; RoboHelp; Domino.doc; CMM/CMMI; ITIL Certification (Foundation in-progress); ISO 12207/15288;

ORACLE: 11.5.10 E-Business Suite Family Pack K; Oracle On-Demand; Oracle Balanced Scorecard 5.1, Oracle Daily Business Intelligence (DBI) 7.1; Daily Financials Intelligence (DFI); Daily Payables Intelligence; Daily Service Intelligence; Daily HR Intelligence; IT Strategy & Plan.

OP SYSTEMS & SUPPORT: OS/VS, MVS, XA; OS/400; DOS/VS, VSE; CMS; TSO/SPF; RJE; VPS; RAPS; VOLLIE; GCOS; TSS; IDS-2; TP; ANSI COBOL; CICS Command Level; FOCUS; VSAM; IMS/DB; DB/2; TOTAL/DB; DM-IV; QUICKJOB; Assembler

DESKTOP DOS; OS/2; Novell; Windows NT/XP, UNIX; BASIC, Visual Basic, C++; DB2/2, SPF/PC, Lotus 123, APPROACH; dBase; Microsoft Office Suite

EDUCATION BA in Mathematics, Rutgers University; MBA, Seton Hall University.

PUBLICATIONS & SEMINARS Details are available (separate document) on request.

- Published 27 articles including a book on evaluating and selecting software packages.
- Conducted over 30 workshops, presentation seminars and training sessions.

REFERENCES Details are available on request.

GIT Project Management Philosophy

Global Information Technology, Inc. is uniquely qualified to provide NSE with the optimal situation: accurate and efficient systems that meet the business functionality required by the end-user. This is accomplished by creating project teams consisting of consultants with a variety of expertise and experience. GIT has many consultants considered to be experts in their fields that include such areas as

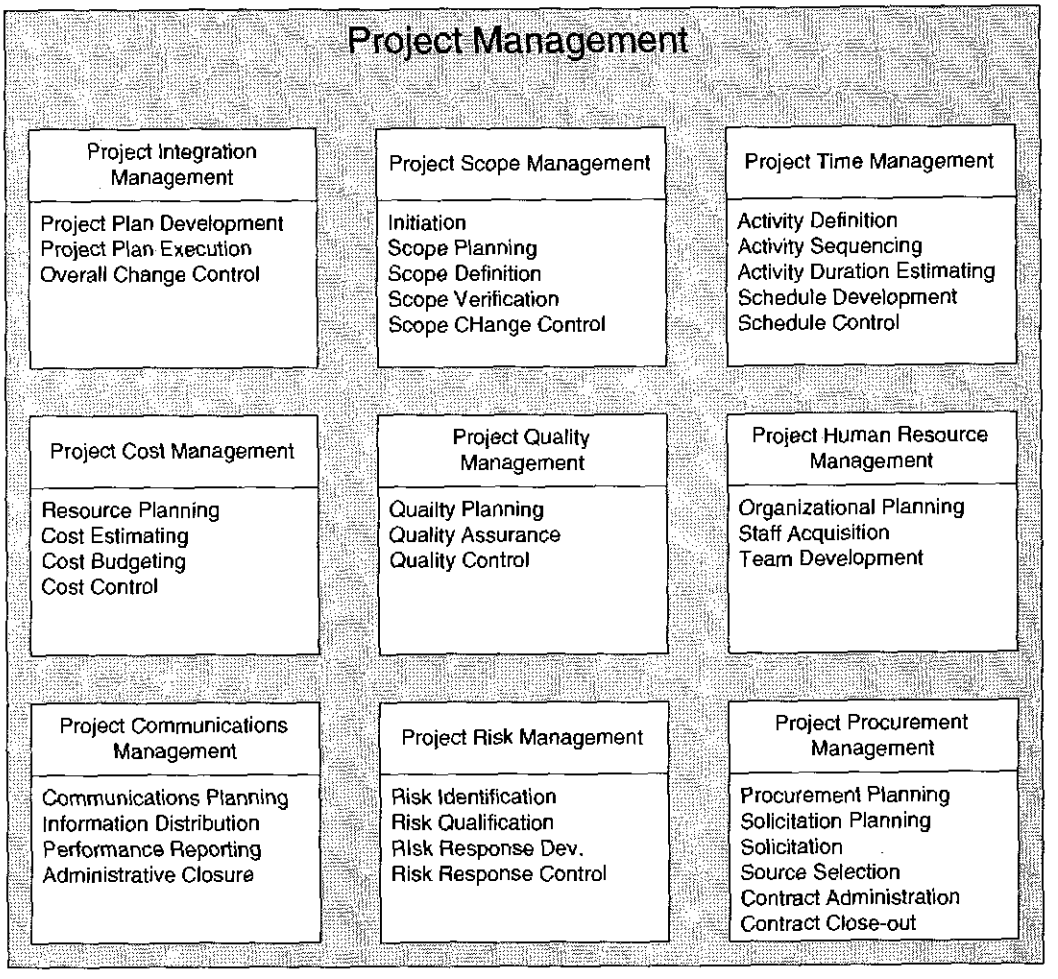
Disaster Recovery Plan and systems backup.

Prior to project initiation, GIT will prepare a "Statement of Work" outlining:

- Project Objectives and Deliverables
- Major Project Activities
- Project Approach
- Roles and responsibilities
- Project Time Line
- Project Reporting and Monitoring Requirements
- Project Assumptions
- Risk Analysis

Project Management Approach

GIT project management is conducted according to standardized processes proven successful on prior GIT engagements. These plans give direction and task overviews to our Project Manager / Team Leads. GIT customizes the Project Management Institute's (PMI) model depicted below for each project.



The key components of GIT Project Management are Planning, Monitoring and Controlling. These are described in further details in the following sections. MS Project will be used to manage these functions when necessary.

Project Monitoring

The key to success is adequate feedback on project status to allow timely and effective resolution of problems that may arise. To ensure project success, GIT will:

- Use a Project Management tool when required.
- Make a distinct definition of intermittent deliverables and milestones.
- Hold weekly Project Team meetings.
- Conduct Technical and Management Reviews.
- Make quick decisions on critical matters to safeguard delivery dates.
- Ensure close coordination between the NSE and GIT.
- Assess and manage risks.
- Conduct internal GIT Management Action Committee meetings.
- Conduct joint NSE and GIT Steering Committee meetings.
- Generate situation reports if required.
- Conduct internal and external continuous improvement meetings.
- Perform scheduled and unscheduled project quality reviews (audits).

Project Reporting

GIT will provide status reports to the NSE at intervals as requested. GIT will provide the NSE a monthly summary of the previous month's activity by the 10th working day. The summary will state the tracking number, invoice number, NSE purchase order number, number of hours worked by specialty, rate, and total amount.

The status report will contain the following:

- An updated Risk Management Plan
- A status of milestones that are due during the reporting period and of milestones that were due during the previous reporting period, but not completed.
- A status of issues described in the previous report.
- A summary of new issues since the most recent report.
- A recommendation and projected date for resolution of issues.
- Summary of accomplishments compared with deliverables schedule.

Project Control

The Project Control procedures to be implemented will help measure progress against plans and management of the resources. These controls include Management Review, Problem Resolution, Risk Management and Change Management.

Management Review

GIT's Project Manager / Team Lead will regularly review status with the NSE and GIT Management to ensure delivery of the project is on schedule with the highest service level. A Steering Committee comprised of NSE and GIT Management will meet monthly for a formal management review.

Project Management Meetings

GIT's project management philosophy is that problems are best solved at the level of the organization where the information to solve it is held. GIT will hold periodic status meetings with appropriate NSE personnel to:

- Review planned versus actual project data
- Identify and resolve issues

- Accept most deliverables
- Prepare joint presentations to the Steering Committee
- Identify Risk Strategies
- Develop alternatives to project threats

It is at this level that most project issues are resolved, with any unresolved issue being presented to the Steering Committee preferably with recommended solutions.

Project Steering Committee

GIT establishes Project Steering Committees for each project GIT manages. This committee provides the second line of project management and provides the next level interface between the NSE and GIT to ensure the project is delivered according to schedule, budget, and quality constraints. This committee will provide the following management tasks:

- Monitor the progress and direction of a specific project
- Represents client and GIT constituencies in decision making process
- Sets overall project direction
- Serves as review and arbitration committee
- Helps overcome obstacles
- Ensures quality of personnel assigned to project
- Reviews major work packets and design decisions

Problem Resolution

A number of problems, issues and concerns are likely to arise during the course of the project. GIT's Project Manager / Team Lead and NSE's Project Manager / Team Lead will engage in regular communication to discuss and resolve problems without delay. In case the problems are not resolved, escalation procedures will be developed involving the Steering Committee.

Risk Management

The GIT Project Manager will identify risks associated with the project and will develop a risk management plan and report against it throughout the life cycle of the project.

Change Management

Either the NSE or GIT may initiate change requests to this Proposal / Statement of Work. Change requests shall be in writing and documented in a clear and concise manner and, to the extent possible, shall contain a good faith estimate of the additional or reduced expense, delay and/or other impact as a result of the proposed change. No work will be performed pursuant to a change request until both parties have approved it in writing.

The Change Management Process is put in place to control the scope of the overall engagement and/or a sub-project of the engagement. It is rare for a project to progress without some change in the plan. If processes are not set to handle change in a structured manner, projects may fail to meet expectations/goals such as budgets, estimates and/or schedules.

The following is an overview of the Change Management Process:

Change Initiation

The NSE or GIT may initiate change Requests. Reasons for a change may include NSE requests, change in scope or other detailed technical issues. Change Requests will be documented in a clear and concise

manner on a Change Request Form. Change Requests will be submitted to the corresponding NSE's Project Manager.

Change Validation

Change Requests shall initially be presented and discussed at project Steering Committee meetings. It is the Steering Committee responsibility to validate and determine whether a cost estimate is needed for the change.

Cost Estimate Preparation

Within an agreed upon number of work days of Steering Committee validation of a Change Request, a cost estimate will be prepared by GIT. GIT will provide an estimate to the organization requesting the change using the same or similar methods to those used in the preparation of the original project estimate and shall fully document the scope of the change, and fully justify all estimated adjustments in price, schedule and/or other factors as applicable.

Change Approval

After estimates are received, the requesting organization will initiate their internal approval process. Once the appropriate approvals and authorizations are obtained, the requesting organizations Project Manager / Team Lead may direct GIT to Implement the Change, Close the Change Request or place the Change on Hold for later implementation. Such direction from the requesting organizations to GIT shall be in writing and shall reference the specific Change Request Form. The requesting organizations acknowledge that if a Change recommended by GIT is rejected, the project may be delayed or possibly may not be completed.

Change Implementation

When a Change Request is authorized by the requesting organizations for implementation, the Change Request Form shall be appended to the Statement of Work for an engagement level change or to the appropriate sub-project documentation. If applicable, a schedule (separate from but integrated with the Project Schedule) shall be developed and maintained for each such authorized Change. Copies of the Schedule shall be delivered to the requesting organizations Project Manager / Team Lead and appropriate project personnel.

If appropriate, GIT shall charge the requesting organizations for the implementation costs defined in the approved Change Request, in accordance with the rate(s) indicated in the Financial Summary of the Statement of Work.

Quality Management Process

GIT has implemented rigorous Quality Control and Quality Assurance procedures for all Development and Support engagements. GIT's Quality Control and Quality Assurance procedures are aimed at ensuring:

- Projects deliver to the requirements.
- Projects are executed within the agreed time frame.
- Projects are executed within the budgeted resources and costs.
- Project deliverables have minimal defects when delivered to the NSE or delivered to the next stage/activity within the project.
- Project deliverables are maintainable and can be enhanced to meet the NSE's changing needs.
- Project deliverables comply with the agreed standards.
- Project Management Methodology is consistent within and across projects.

- Defect information and resolutions are shared across projects with similar technologies.

GIT distinguishes Quality Control from Quality Assurance procedures. Quality Control activities ensure that deliverables meet the required quality level. Quality Assurance activities ensure that procedures, structures and standards laid out for engagements are conducive to delivering quality deliverables and that these procedures, structures and standards are implemented in all deliverables.

Quality Control

Quality Control activities for the projects will be characterized by the following:

- They form a part of the project execution activities.
- They will be identified during initial segments in the form of a Project Quality Control Plan.
- They will be carried out on deliverables such as the Requirement Document, Architectural Specification, Technical Specification, Design Documents, Program Specifications, Program Code, System Testing, etc. (as appropriate).

Quality Assurance

Quality Assurance at GIT is an overall organizational activity and will be carried out as a matter of course on this project. GIT's Quality Assurance process includes the following characteristics:

- Becomes the foundation for organization-wide standards and procedures.
- Verifies that every Project Management Plan and Quality Control Plan, when implemented will result in deliverables of high quality.
- Authorizes project specific standards and procedures that deviate from GIT's organizational standards and procedures.
- Ensures that organizational and project specific Quality Control standards are being followed.
- Verify that the Quality Control standards used by projects are resulting in the desired quality level in project deliverables.
- Confirms that the Project Management and Control procedures and standards are being followed.
- Collects project statistics for improvement in processes and also for using as the historical basis for enhancing the accuracy of future estimates.

Quality Review Process

Quality Assurance/Quality Control Reviews will be GIT's formal mechanism of implementing Quality Assurance and Quality Control procedures at the NSE. Irrespective of the deliverable/process under review, the following steps will be followed:

- **Initiate the Review**: All members of the review team are informed of the date, time and purpose of the review. The members of the review team are also provided with all the background material necessary to conduct the review.
- **Conduct the Review**: The members of the review team conduct the review and document defects/comments.
- **Consolidate Review Comments**: The moderator of the review decides on the actions that are needed to address the comments and defects found by the review team. The moderator may discuss the comments and defects with the author and members of the review team before deciding on the actions. The moderator also decides on the need for a follow up review.
- **Implement Action Plan to Achieve Compliance**: The review action points are placed into an action plan and that plan is approved and executed.

3.3 Key Personnel

Key Personnel, for Reference:

Job Title	Name	Telephone	Email
Executive President	Suren K. Ajjarapu	813.601.3533	sajjarapu@git-org.com
Vice President	Tom Iseghohi	202.714.0624	TomIseghohi@aol.com
Delivery Director	Mike Ike	901.218.6233	mikeike99@gmail.com
Project Manager	Irv Brownstein	908.872.8139	irvtpg@yahoo.com
DR Technical Architect	Michael Powers	210-679-7242	Powers.mt@gmail.com
Network Engineer	Tony Williams	727-783-2345	Tsm89@aol.com
Security Administrator	Allan Colaco	813-973-6578	acollaco@citigroup.com
Database Administrator	Siva Kumar	813-604-2635	skumar@citigroup.com
Telecom Engineer	Robert Ward	813-985-2356	Rward72@yahoo.com

3.4 Project Monitoring and Status Reporting

GIT proposes that our project manager shall monitor all activities performed during all stages of this project. We will utilize Microsoft Project as the tool to create, update, and manage all project plans in all phases of this project. An issue log will be maintained and tracked, including all action items related to the issues.

Issues that affect the critical path activities for any stage will be brought to the attention of the NSE's liaison to our project in order to ensure these critical issues receive proper management visibility.

Project status reporting will occur formally once per month on the first business day of the month for the preceding month's activities. In addition, there will be a final status report at the end of each stage.

GIT will:

- Track the status of all pertinent issues and will provide current status of associated action items, staff assigned to work the issue, and possible impacts on schedule and cost.
- Compose a monthly status report detailing progress on activities, progress on issue resolution, costs incurred for the period and costs to date on the stage
- Provide information regarding schedule, effort changes
- Provide updated Microsoft Project plans with changes to planned activities noted and status and percent completed on tasks.

4.0 SECTION 4: TECHNICAL APPROACH AND WORK PLAN

4.1 Overview and Background

The Nigerian Stock Exchange (NSE) invited submission of qualifications and proposal data (collectively referred to as the "Proposal") from interested U.S. firms which are qualified on the basis of experience and capability to develop a technical assistance program to assist in the development of a disaster recovery plan for the Nigerian Stock Exchange (NSE).

NSE and its management team understands the importance of a reliable stock exchange and thus, has requested the U.S. Trade and Development Agency (USTDA) assistance to a disaster recovery plan which will provide a mechanism for continuous trading and support of the NSE in case of failure of the main building or main equipment and ensure that the data stored and transferred on the NSE's hardware and communications infrastructure is fully recoverable and secure.

4.1.1 Scope

The basis for the content of this proposal is the document titled "NSE Terms of Reference".

NSE Technical Assistance will include:

- The review of existing IT systems and plans, existing hardware and communications infrastructure, and
- Developing a strategic plan, specifications, and an implementation plan for a disaster recovery facility.
- Ensuring that any recommended procurements can be integrated with existing hardware, communications infrastructure, applications, and databases.

The NSE would also like to use this Technical Assistance to:

- Obtain Security, Reliability, and Data Integrity certification of the exchange. The NSE currently does not have a full accounting of its security-related infrastructure.
- Identify existing physical and IT infrastructure security operations and gaps at the NSE, and
- Develop a strategic plan for security at the disaster recovery facility.

The primary scope of the work to be performed under this proposal is to:

- Produce the DR Report as appropriate for the NSE environments
- List the time criteria for restoring the NSE's operating environment
- Document the provisions for recovery of mission critical IT processing capabilities and Applications within the time frames provided by the plan.

This project does not include funds to:

- Purchase any software tools or packages that may be recommended as a result of work on this project.
- Perform tests of the effectiveness of the disaster recovery procedures documented in the plan
- Conduct or support any new/modified Vendor Agreements
- Negotiate or support any new/modified internal Agreements
- Perform training on any selected and implemented tools.

When completed, this project will have successfully documented the upgraded plan (TCBP).

4.1.2 Current NSE Business & Environment

NSE was established in 1960 and currently has some 282 listed companies with a total market capitalization as at the end of 2005 of around $20 billion. All listings are included in the only index, the Nigerian Stock Exchange All Shares Index. The Exchange, made up of 10 Government Stocks, 55

Industrial Loan (Debenture/Preference) Stocks and 195 Equity / Ordinary Shares of Companies. Most of the listed companies have foreign/multinational affiliations and represent a cross-section the economy, ranging from agriculture through manufacturing to services.

The Lagos Exchange is an affiliate member of the Federation of International Stock Exchanges (FIBV). It is also an Observer at meetings of International Organization of Securities Commissions (IOSCO), and a foundation member of the African Stock Exchanges Association (ASEA).

The Exchange has an Automated Trading System. Data on listed companies' performances are published daily, weekly, monthly, quarterly and annually.

NSE Overview

Nigerian (Lagos) Stock Exchange	
Types of Securities Traded:	Shares, Government Bonds, Corporate Bonds
Forms of Securities:	Physical to be immobilized in 1997
Trading System:	Call - over/open outcry
Trading Hours:	Monday - Friday 11:00-13:00
Supervisory Body:	Securities & Exchange Commission
Clearing & Settlement Organization:	Central Securities Clearing System (CSCS)
Settlement Cycle:	T + 3
CSD:	CSCS
Taxes on Transaction:	3% commission on the traded value of shares and a 1% Securities and Exchange Commission fee
Taxes on Dividend and Interest:	Withholding taxes on Dividend is 10% / Capital Gain tax 10%; Corporate Income tax is 35%

NSE Trading:

The call over trading system was in April replaced with the Automated Trading System (ATS), with bids and offers now matched by stockbrokers on the Trading Floors of The Stock Exchange through a network of computers. This is done every business day from 11.00 a.m. till all bids and offers have been executed (about 1.30 p.m. on the average).

NSE Pricing:

Prices of new issues are determined by issuing houses/stockbrokers, while on the secondary market prices are made by stockbrokers only. The market/quote prices, along with the All-Share Index, are published daily in The Stock Exchange Daily Official List, The Nigerian Stock Exchange CAPNET (an intranet facility), The Nigerian Stock Exchange website (www.nigerianstockexchange.com), Newspapers and on the stock market page of the Reuters Electronic Contributor System. Our on-line code in the Reuters Network is NSXA-B.

The All-Share Index:

The Exchange maintains an All-Share Index formulated in January 1984 (January 3, 1984 = 100). Only common stocks (ordinary shares) are included in the computation of the index. The index is value-relative and is computed daily.

NSE Clearing, Delivery and Settlement:

Clearing, Settlement and Delivery of transactions on The Exchange are done electronically by the Central Securities Clearing System Limited (CSCS), a subsidiary of The Stock Exchange. The CSCS Limited ("the Clearing House") was incorporated in 1992 as part of the effort to make the Nigerian stock market more efficient and investor-friendly. Apart from clearing, settlement and delivery, the CSCS Limited offers custodian services.

NSE Regulation:

Transactions on The Exchange are regulated by The Nigerian Stock Exchange, as a self-regulatory organization (SRO), and the Securities & Exchange Commission (SEC), which administers the Investments & Securities Decree 1999.

4.1.3 Work Approach

The project will address each area of the Terms of Reference (Noted below) in the NSE DR Development Plan:

- Review Existing IT Systems and Plans
- Review Backup, Recovery, and Security-Related Operations and Business Procedures
- Current State Assessment Document and Presentation
- Identify DR Strategic Plan and System Requirements
- Identify DR System Specifications
- Develop Implementation Plan
- Document Supplier Identification
- Development Impact Analysis
- Preliminary Environmental Impact Assessment
- Working Group Meeting and Presentation
- Document Final Report

The project incorporates the Terms of Reference into seven (7) broad segments of work described in the NSE DRP Development Plan section.

GIT proposes to break the project into seven (7) stages:

1. DR Data Gathering & Current State Assessment
2. Document Emergency Response Procedures
3. Document Plan Activation Procedures
4. Document Administrative Procedures
5. Document Key DR Reports
6. Document Key DR Forms

7. Final Delivery & Reporting

A summary of Deliverables is provided in the final sub-section.

The GIT Project Team will work directly with the NSE liaison to complete the project.

GIT expects Stage I to start on or about 11 September 2006 and be completed on or about 29 December 2006.

4.2 DR Data Gathering & Current State Assessment

GIT will complete this stage of the project in three tasks:

	Task Summary
1	Identify key Areas/individuals
2	Distribute/Conduct Data Gathering Template(s)
3	Complete Gap Analysis & DR Assessment

4.2.1 Identify key Areas/individuals

Working with the NSE liaison, the Project Team will:

- Identify all relevant areas within the Project Scope,
- Identify all relevant individuals within the Project Scope
- Identify all relevant functions within the Project Scope
- Identify all relevant projects within the Project Scope
- Identify all relevant existing materials and prior DR approaches.

4.2.2 Distribute/Conduct Data Gathering Template(s)

The Project Team will utilize a combination instruments (both on-site and off-site) and Templates (see Appendix) to complete data gathering. Our activities include:

- Administer DR Procedure Templates and Forms to a wide range of stakeholders and Subject Matter Experts working with the NSE liaison
- Conduct formal interviews with key personnel selected in consultation with the NSE liaison
- Review current documentation and records identified by the NSE liaison for:
    - IT Systems and Plans
    - Mission Critical Processes
    - Backup, Recovery and Security Related Operations & Business Procedures
- Observe current process operations and engage in informal interviews
- Determine key NSE processing and operational constraints.

4.2.3 Complete Gap Analysis & DR Assessment

Here, the GIT Project Team will:

- Analyze objective and subjective data from all assessment activities
- Compare findings to GIT and industry standards to provide an NSE DR Gap Analysis
- Prepare an interim DR Assessment report of our findings,
- Present the Current State DR Assessment findings to NSE.

4.3 Document DR Emergency Response Procedures

GIT will complete this stage of the project in three tasks:

	Task Summary
1	Emergency Evacuation Procedures
2	Emergency Phone Numbers
3	Emergency Notification Procedures

4.3.1 Emergency Evacuation procedures

The safety and security of employees is of the highest priority. Evacuations will be announced verbally and designated Evacuation Personnel will proceed with overseeing their department's evacuation.

Document the emergency procedures that are to be used to evacuate all NSE employees in case of:

- A building fire,
- Tornado,
- Earthquake or
- Bomb threat.

The Evacuation Personnel from various departments will assist with the evacuation of all employees from the facility.

4.3.2 Emergency Phone Numbers

Identify and Document All Phone Numbers per Category.

For example: "Category – Fire; Telephone No: XXX

4.3.3 Emergency Notification Procedures

Document the emergency notification procedures that outline the communications path during different levels of an outage.

For example:

- In the event of a regional outage the local number automatically rolls to a backup location (TBD) if all phones are logged off the system.
- If all phones are not logged off the system, call (TBD) to have the number re-routed.

4.4 Document DR Plan Activation Procedures

GIT will complete this stage of the project in ten (10) tasks:

	Task Summary
1	Activate Incident Management Team
2	Activate Emergency Operations Center
3	Emergency Declaration Procedures

	Task Summary
4	Relocate Operations Procedures
5	Situation & Damage Assessment Procedures
6	Communications
7	Offsite Storage
8	Purchasing procedures
9	Recovery Site Generator, Electrical & Security plan Procedures
10	Reconstruction Procedures

4.4.1 Activate Incident Management Team

Document the Team Composition Report and ensure that all required Incident Management Team Members are present at the Emergency Operations Center.

Document procedure and ensure that Contact recovery personnel are contacted in the correct order:

4.4.2 Activate Emergency Operations Center (EOC)

Document the Emergency Operations Center procedures ensuring that they address obtaining necessary resources, and performing the following tasks:

- Document the Team Composition Report
- Ensure that the EOC conference room has adequate phones and fax machines.
- Ensure 7 am – 8 PM CST phone coverage, and log all incoming calls.
- Maintain the status of functions and personnel that have been relocated. Utilize the Personnel Location Control Form.
- Maintain a log of recovery activities.
- Distribute the purchasing procedures and Time Sheet Tracking Form to all recovery personnel.
- Ensure compliance with all of the Administrative Procedures.
- Ensure that directions to the EOC are current
- Keep appropriate levels of management informed.

4.4.3 Emergency Declaration Procedures

Document the Emergency Declaration procedures ensuring that they address:

- Only the Incident Management Team (IMT) Leader or Alternate Team Leader has the authority to
  - declare an emergency and
  - the subsequent relocation of the technology environments and/or the end user workspace to the designated recovery location
- Review all available information regarding the incident including the Damage Control Status Report;
- Work with the appropriate members of the City and the IMT to make the decision to declare an emergency and relocate operations;
- Communicate the decision to all members of the IMT and Communications Team prior to the emergency declaration;
- How to declare an emergency

4.4.4 Relocate Operations Procedures

Document the Relocate Operations procedures ensuring that they address:

- Notifying all critical personnel to report to the EOC per the IT Contacts Report and the Business Unit Contacts Report for critical personnel contacts information.
- The EOC facility has available required workspace, accesses & resources per Setup Checklist and pre-defined floor layout diagrams
- Key steps are identified for action immediately after relocation. For example:
  - Immediately begin wiring of workspace and data room to the existing generator.
  - Set up of area furniture.
  - Contact to install Telephones.
  - Provide a map of available equipment (Fax machines, Copiers, etc.) to critical personnel.

4.4.5 Situation & Damage Assessment Procedures

Document the Relocate Operations procedures ensuring that they address:

- The Situation and Damage Assessment Team Leader or Alternate Team Leader selects appropriate personnel to travel to the damaged site to assess the damage.
- Once on site the Team should follow the updated decision matrix to determine if they should or should not enter the damaged facility.
- Conduct the Damage Assessment Inspection

4.4.6 Communications

Document the Communications procedures ensuring that they address:

- All Communications will be handled by the Communications Team Leader and/or Alternate Team Leader
- Obtain key status information either from the EOC or directly from the Situation and Damage Assessment Team if the EOC has not been convened.
- Ensure that the overriding message communicated is that the company has met the crisis, are dealing with it and normalizing operations in line with the technology business continuity plan.
- Directly manage all relations following a business disruption. Communications may ask other individuals to respond to media inquiries, but this will only occur if specifically requested by a Communications representative.
- Keep a documented log of all incoming and outgoing communications.
- Actively manage all post event communications.
- Be consistent with updated Communication Do's & Don'ts List

4.4.7 Offsite Storage

Document the Offsite Storage procedures ensuring that they address:

- The Off Site Storage Team is the control and coordination point for the retrieval and delivery from off site storage of all vital records (including backup tapes), documentation and equipment to the recovery location.
- Directions to the Off-site Storage location(s)
- Inventory items stored at each location
- The Off Site Storage Team will be responsible for the distribution of all vital records and equipment to Technology Recovery Teams at the recovery location(s). Members of the Off Site Storage Team, as determined by the Off Site Storage Team Leader

4.4.8 Purchasing procedures

Document the Purchasing procedures ensuring that they address:

- In the event a disaster and significant damage has occurred to critical equipment and supplies, the policy and procedure that will be placed into effect.
- What process will remain in effect during a disaster recovery period?
- What exception to current operating procedures that will be in force.
- How the immediate need for critical replacement equipment, the process of obtaining quotes will need to be suspended and handled.
- This change to current operating procedures will only be in effect if a disaster has been declared by the City and will remain in effect until critical replacement equipment and supplies have been procured.

4.4.9 Recovery Site Generator, Electrical & Security Plan Procedures

Document the Recovery Site procedures ensuring that they address the needs of a viable recovery site that will need to be addressed at the facility. They include:

- Replacement of the existing generator with a larger capacity model to support the entire facility in the event of a power outage.
- Installation of electrical wiring to support the backup data equipment located in the receiving area, generator upgrade support and electrical outlets in the larger classroom area to support recovery personnel.
- Upgrade the existing security to the facility to protect backup equipment located in receiving area, to include caging as required.

4.4.10 Reconstruction Procedures

Document the Reconstruction procedures ensuring that they address:

- The Reconstruction Team will meet with Insurance to review insurance coverage and options, requirements, documentation, and procedures associated with filing the insurance claim to ensure reimbursement of loss amounts.
- Develop a preliminary high level restoration plan for the location,
- Meet with the Business Units or Technology Recovery Teams to review the preliminary restoration plan for the location:
- Once a strategy is approved for the restoration of the location, expand the restoration plan for the location.
- Work with the Technology Recovery Teams to develop an equipment installation and move plan.
- Work with the Incident Management Team on any insurance related issues.
- Keep the Incident Management Team apprised of the status on all facility, equipment and construction activities, including equipment salvage activities.
- Participate in an advisory role in the activation of the move back to the repaired data center.

4.5 Document DR Administrative Procedures

The administrative responsibilities summarize NSE policy. These responsibilities and procedural guidelines must be applied throughout the initial response and any subsequent business recovery activities.

	Task Summary
1	Enforce NSE Policies

	Task Summary
2	Monitor & Report Recovery process
3	Maintain Recovery Related Record Keeping
4	Define Testing & Maintenance Functions

4.5.1 Enforce NSE Policies

Document the Enforce NSE Policy procedures ensuring that they address:

- Monitor security and control policies and procedures.
  - Experience indicates that companies are particularly vulnerable to fraud and sabotage during times of disruption.
  - Obtain, from the Incident Management Team, approvals for any changes to standard control policies.
- Maintain emergency-related expense tracking and controls.
  - All expenses incurred as the result of business recovery may need to be charged to a special cost center code established at the time of the business disruption.

4.5.2 Monitor & Report Recovery process

Document the Recovery procedures ensuring that they address:

- Monitor the recovery progress frequently (hourly the first day - minimally daily thereafter).
- Collect written status reports from recovery teams daily.
- Submit verbal and written status reports to the Incident Management Team on a similar basis.

4.5.3 Maintain Recovery Related Record Keeping

Document the Recovery Record-Keeping procedures ensuring that they address:

- Maintain careful written records throughout the recovery process.
- Experience shows that thorough and complete records are invaluable in reducing confusion during the recovery and in reconciling material acquisitions and expenses.

4.5.4 Define Testing & Maintenance Functions

Document the Testing & Maintenance Function procedures ensuring that they address:

- All NSE operating & performance criteria
- All NSE maintenance criteria
- All NSE security criteria

4.6 Document Key DR Reports

The Reports are a critical mechanism for communication throughout and after the Disaster/Recovery period.

	Task Summary
1	Business Unit Key Contacts
2	Summary of Critical Applications, Servers & RTO's

	Task Summary
3	Vendors & Suppliers
4	Summary of Desktop & Workspace Requirements
5	Other Equipment
6	Critical Telephone Numbers Report

4.6.1 Business Unit Key Contacts

Focus: End User Contacts & Locations Recovery Time Objectives

Action: Document the report's content, input and distribution.

4.6.2 Summary of Critical Applications, Servers & RTO's

Focus: Specific Application & Servers Recovery Time Objectives

Action: Document the report's content, input and distribution.

4.6.3 Vendors & Suppliers

Focus: Identify all Vendors & Suppliers – Key Contacts, Services & Contact Information

Action: Document the report's content, input and distribution.

4.6.4 Summary of Desktop & Workspace Requirements

Focus: Specific Workspace Needs such as Telephone Recovery Time Objectives

Action: Document the report's content, input and distribution.

4.6.5 Other Equipment

Focus: Specific Workspace Needs such as local Printer Recovery Time Objectives

Action: Document the report's content, input and distribution.

4.6.6 Critical Telephone Numbers Report

Focus: Specific Critical Telephone Recovery Time Objectives

Action: Document the report's content, input and distribution.

4.7 Document Key DR Forms

The Forms are a critical support provided to all Recovery Teams for use throughout and after the Disaster/Recovery period.

	Task Summary
1	Recovery Activities Log
2	Critical Files & In-Progress Assessment
3	Critical Equipment & Assessment

	Task Summary
4	Personnel Locations Control Form
5	Time Sheet tracking
6	Telephone Log
7	Damage Control Status
8	Bomb Threat Response
9	Injury Status Reporting
10	Receiving Room Sign-In

4.7.1 Recovery Activities Log

Focus: Track Activities
Action: Document the form's content, input and distribution.

4.7.2 Critical Files & In-Progress Assessment

Focus: Assess & Evaluate Critical Files & Work In-Progress
Action: Document the form's content, input and distribution.

4.7.3 Critical Equipment & Assessment

Focus: Assess & Evaluate Critical Equipment
Action: Document the form's content, input and distribution.

4.7.4 Personnel Locations Control Form

Focus: Maintain Centralized Control of all Recovery Personnel
Action: Document the form's content, input and distribution.

4.7.5 Time Sheet tracking

Focus: Track Allocation of Time per person by week
Action: Document the form's content, input and distribution.

4.7.6 Telephone Log

Focus: Track Incoming Telephone Calls
Action: Document the form's content, input and distribution.

4.7.7 Damage Control Status

Focus: Checklist for Damage Control Assessment plus Narrative Status Assessment
Action: Document the form's content, input and distribution.

4.7.8 Bomb Threat Response

Focus: Checklist for Documenting Bomb Threats
Action: Document the form's content, input and distribution.

4.7.9 Injury Status Reporting

Focus: Track Injury Status Activities
Action: Document the form's content, input and distribution.

4.7.10 Receiving Room Sign-In

Focus: Track Receiving Room In/Out Activities
Action: Document the form's content, input and distribution.

4.8 Final Delivery & Reporting

The implementation plan and Final Report are key to completing the project.

	Task Summary
1	Develop DR Implementation Plan
2	Document & Deliver Final DR Report
3	Conduct Final DR Presentation

4.8.1 Develop DR Implementation Plan

Develop the detailed DR Implementation Plan outlining:

- Steps to implement the Recovery Site
- Steps to manage Suppliers
- Steps to determine and negotiate software, hardware, resources, facilities needs
- Steps to define, execute and evaluate "fire-drills."

4.8.2 Document & Deliver Final DR Report

Document and organize DR materials into one or more volumes:

- Establish Change Management procedure
- Prepare Master copy for ongoing maintenance
- Prepare Distribution copies as appropriate

4.8.3 Conduct Final DR Presentation

Prepare MS PowerPoint presentation that addresses:

- Project parameters
- NSE DR Report delivery
- NSE DR next steps.

4.9 NSE DR Deliverables Summary & Schedule

The table below shows the schedule of deliverables by stage of the project.

	Section 4 Stage	Deliverable(s)	Schedule
1	DR data Gathering &	• NSE Current State DR Assessment	Sept 2006

	Section 4 Stage	Deliverable(s)	Schedule
	Current State Assessment		
2	Document DR Emergency Response Procedures	• Emergency Evacuation Procedures • Emergency Phone Numbers • Emergency Notification Procedures	
3	Document DR Plan Activation Procedures	• Activate Incident Management Team • Activate Emergency operations Center • Emergency Declaration Procedures • Relocate Operations Procedures • Situation & Damage Assessment Procedures • Communications • Offsite Storage • Purchasing procedures • Recovery Site Generator, Electrical & Security plan procedures • Reconstruction Procedures	Sept / Oct 2006
4	Document DR Administrative Procedures	• Enforce Company Policies • Monitor & Report Recovery process • Maintain Recovery Related Record Keeping	Sept / Oct 2006
	Document DR Reports	• Business Unit Key Contacts • Summary of Critical Applications, Servers & RTO's • Vendors & Suppliers • Summary of Desktop & Workspace Requirements • Other Equipment • Critical Telephone Numbers Report	Nov / Dec 2006
6	Document DR Forms.	• Recovery Activities Log • Critical Files & In-Progress Assessment • Critical Equipment & Assessment • Personnel Locations Control Form • Time Sheet tracking • Telephone Log • Damage Control Status • Bomb Threat Response • Injury Status Reporting • Receiving Room Sign-In	Nov / Dec 2006
7	**Final Delivery & Reporting**	• **DR Implementation Plan** • **Final DR Report Master** • **Final DR Presentation**	**Dec 2006**

5.0 SECTION 5: EXPERIENCE AND QUALIFICATIONS

5.1 Experience and Qualifications

DR Technical Architect

Edward (Ed) F. Sanderson - Status: U.S. Citizen
Address: *5161 Cote du Rhone Way, Sarasota Fl 34238* – **Cell Phone**: 941.320.6701
Phone: *941-922-8446* - **email:***consulting@sdsecure.com* - **web:***www.sdsecure.com*
Providing compliance, data administration information security and disaster recovery/business continuation consulting services to a broad range of corporate clients.

Summary

As an Information Technology professional I have strong, Project Management, Data Administration, Identity Management, Information Security, Compliance & Sarbanes-Oxley Regulatory Compliance and Disaster Recovery/ Business Continuation experience. This background includes proficiency in the development, documentation and implementation of regulatory, information security, disaster recovery, and business continuity solutions for the distributed environment.

Professional Experience

Project Title:	**DR/BCP and Information Security Analysis**
Client:	A&P Montvale, New Jersey.
Duration:	March 2002 – January 2003
Role:	Security Analysis
Software/Tools:	Microsoft Office, MS Project, Windows 2000, AIX, RACF

Description:

- **Disaster Recovery/Contingency Planning** Developed data privacy policy and standards for test data using company PII standards that were compliant to ISO standards.
- **Disaster Recovery/Contingency Planning** Developed business contingency planning and disaster recovery policy and procedure framework.
- **Security:** Performed detailed security and access control analysis of Oracle Financial system being implemented. Created access control strategy focusing on Segregation of Duties for Accounts Receivable, Accounts Payable, and General Ledger and Fixed Asset modules.
- **Security:** Developed business case, security architecture, and process implementation for an Identity Management process.
- **Security**: Developed business case, security architecture, and process implementation for an Identity Management process. The components included the identification, selection and piloting of Provisioning, Web Access Control, and role based solutions.
- **Security**: Developed end-to-end strategies for on-boarding requirements for consultants and employees.

Project Title:	**Information Systems Disaster Recovery**
Client:	Pfizer (Agouron), San Diego, CA
Duration:	March 2001 – June 2001
Role:	Project Lead
Software/Tools:	Microsoft Office, UNIX and NT

Description:

- **Disaster Recovery/Contingency Planning** Reviewed and recommended modifications to FDA process validation criteria.
- **Disaster Recovery/Contingency Planning** Developed a disaster recovery plan for a large international distributed information technology environment based on 21 CFR Part 11 requirements.

Project Title:	**E-Commerce Information Security Analysis and Implementation**
Client:	Merrill Lynch Bank USA, Plainsboro, New Jersey
Duration:	May 2000 – August 2000

Role: Project Coordinator
Software/Tools: Microsoft Office, Microsoft Project, UNIX and NT, PentaSafe, Bindview, Globus

Description:

- **Disaster Recovery:** Updated and tested a disaster recover program for the Globus Banking system.
- **Security:** Performed risk and gap analysis to identify access control issues and remedies.
- **Security:** Perform product review and selection of UNIX/NT audit and administration products.
- **Security:** Performed security review of e-commerce banking applications.
- **Security:** Participated in a re-engineering review of application functionality by role.
- **Security:** Reviewed implementation of Globus Applications for Merrill Lynch Banking Application with a focus on security and roles and responsibilities.

Project Title: **Disaster Recovery/Business Contingency Planning**
Client: Chase H & Q, San Francisco CA
Duration: November 1999 – April 2000,
Role: Project Manager
Software/Tools: Microsoft Office, Microsoft Project, Visio, UNIX and NT, PKI Software, Intranet and Internet Networking

Description:

- **Disaster Recovery/Contingency Planning** Developed, documented and rolled out detailed plans to establishing business contingency strategies for Information Technology and brokerage business units in a distributed Sun Microsystems UNIX and NT web based Internet and Intranet environment.
- **Disaster Recovery/Contingency Planning** – Leveraged Strohl Systems LDRPS Disaster Recovery tools to create plan.

Project Title: **Disaster Recovery/Business Contingency Project Coordinator**
Client: INTELSAT, Washington D.C
Duration: April 1999 – November 1999
Role: Project Manager
Software/Tools Microsoft Office, Microsoft Project, Visio, UNIX and NT, Sungard

Description:

- **Disaster Recovery/Contingency Planning:** Developed and documented disaster recovery and business continuity strategies and plans for all departments in a global distributed environment.
- **Disaster Recovery/Contingency Planning** Developed recover strategies for applications using Oracle database.
- **Disaster Recovery/Contingency Planning:** Used Sungard Recovery tool to create plan.

Project Title: **Vision 2000 Security Architecture**
Client: Guardian Life Insurance Company
Duration: New York City, September 1997 – April 1999
Role: Project Manager Implementer
Software/Tools: RACF, Proxima SSO, Tivoli Unix, NT, Firewalls

Description:

- **Security:** Created and documented security policies and procedures to be used to control and administer security in a commercial web application environment.
- **Security :** Project manager for a Single Sign-on product in a large multi-platform environment.
- **Security:** Participated in a detailed re-engineering analysis of job function and automated application requirements.

Project Title: **Contingency Plan Review**
Client: Metropolitan Water District Of Southern California, Los Angeles, and Calif.
Duration: June 1996

Role: Contingency Planning Consultant
Software/Tools: Microsoft Office

Project Title: **Business Contingency Planning**

Client: ***Putnam Investments, Boston, and Ma***
Duration: February 1996 to May 1996

Role: Disaster Recovery Consultant
Software/Tools: UNIX SUN, Microsoft Office
Project Title: Disaster Recovery/Business Continuity Planning
Client: Disclosure, Inc. Beheads, MD
Duration: October 1995 to January 1996

Role: Disaster Recovery Consultant

Client: 24 Hour Fitness, Carlsbad, CA
Project Title: Identity Management Analyst
Duration: January - February 2006
Role: Information Security Classification and Identify Management Lead
Software/Tools: Microsoft Office, MS Project, MS Client Server, Oracle Financials

- **Identify Management:** Analyze existing access entitlements of Oracle Financials responsibilities by user job roles.
- **Identify Management:** Establish user access criteria for segregation of duties based upon existing Oracle Financial responsibilities.
- **Identify Management:** Identify and remediate user entitlements where access did not conform to established access criteria.

Client: Hovnanian Builders, New Jersey
Project Title: Process and Compliance Subject Matter Expert
Duration: March 2005 – December 2005
Role: Security and Change Management Compliance and Process Management
Software/Tools: Microsoft Office, MS Project, MS Client Server, Oracle Financials, JDEdwards

- **Change Management**: Performed detailed review and testing of security and change management process for corporate and subsidiary business units from both a business and technology perspective.
- **Change Management**: Developed System Life Cycle strategies, policies, and procedures focusing on distributed management accountability controls for JDEdwards and industry specific ERP Systems. The audit programs focused on change management and security for Accounts Receivable, Accounts Payable and General Ledger process and segregation of duties functions. Tested implemented ERP strategies and developed detailed Gap analysis and remediation plan.
- **Change Management**: Participated in an exercise to leverage Rational ClearCase methodology as a software manager of ERP's solutions in various business subsidiaries.
- **Change Management**: Used Rational ClearQuest for tracking processing defects identified during SOX testing.
- **Disaster Recovery/Contingency Planning**: Planned, coordinated and executed the recovery of financial ERP systems for participating business units on both Windows and Unix platforms.
- **SOX & Compliance:** Performed Sarbanes-Oxley process and analysis for autonomous business unit's base don CobiT/COSO Model.
- **SOX & Compliance:** Assisted units in developing and implementing processes that addressed compliance issues and process efficiencies.

Client: Patriot Transportation, Jacksonville, FL/Baltimore, MD
Project Title: Compliance Subject Matter Expert
Duration: January - March 2005
Role: Security and Change Control Remediation and Compliance Subject Matter Expert
Software/Tools: Microsoft Office, MS Project, MS Client Server, SQL Server, Epicor

- **Change Management**: Performed detailed review and testing for an Epicor ERP system for Accounts Receivable, Accounts Payable and General Ledger functions focusing on access control and authentication across all infrastructure layers.
- **Disaster Recovery/Contingency Planning**: Planned, coordinated, executed and documented. the recovery of financial ERP systems for a Windows platform.
- **Security**: Developed remediation plan and assisted in the development of project plans, procedures and controls to remedy gaps.
- **SOX & Compliance**: Perform detailed Gap Analysis, developed remediation strategies and project plans.
- **SOX & Compliance:** Prepared Sarbanes-Oxley audit review and testing *IT Operations, Security and* Change Management Controls using CobiT//COSO model.

Client: **Spanish Broadcasting Company, Coconut Grove, Fl**
Project Title: SOX Regulatory Compliance SME
Duration: December 2004
Role: Security and Change Control Remediation and Compliance
Subject Matter Expert
Software/Tools: Microsoft Office, MS Project, MS Client Server, SQL Server, Oracle Financials

- **Change Management**: Developed System Life Cycle strategies, policies, and procedures focusing on distributed management accountability controls for JDEdwards and industry specific ERP Systems.
- **Disaster Recovery/Contingency Planning**: Planned, coordinated, executed and documented. the recovery of financial ERP systems for a Windows platform.
- **Security:** Performed detailed review for a large Oracle Financial environment focusing on access control and authentication across all infrastructure layers.
- **SOX & Compliance**: Prepared Sarbanes-Oxley audit for IT Operations, Security and Change Management Controls using CobiT//COSO model.
- **SOX & Compliance:** Perform detailed Gap Analysis, developed remediation strategies and project plans.

Client: **Equity One, Miami, Fl**
Project Title: SOX Regulatory Compliance SME
Duration: September - November 2004
Role: *Security and Change* Control Remediation and Compliance
Subject Matter Expert
Software/Tools: Microsoft Office, MS Project, MS Client Server, SQL Server

- **Change Management**: Performed detailed review for a large J. D. Edwards environment focusing on access control and authentication across all infrastructure layers.
- **Disaster Recovery/Contingency Planning**: Planned, coordinated, executed and documented. the recovery of financial ERP systems for a Windows platform.
- **SOX & Compliance**: Prepared Sarbanes-Oxley audit for IT Operations, Security and Change Management Controls using CobiT//COSO model.
- **SOX & Compliance**: Perform detailed Gap Analysis, developed remediation strategies and project plans.
- **SOX & Compliance**: Interfaced with external auditors to validate documentation and resolve Sarbanes-Oxley compliance issues.
- **SOX & Compliance**: Created tests using CobiT framework model as a guideline.

Client: **UPS, Mahwah, New Jersey**
Project Title: Sarbanes-Oxley Compliance
Duration: July 2004 – August 2004
Role: Sarbanes-Oxley SME
Software/Tools: Microsoft Office, MS Project

- **Security-Change Management:** Perfromed Gap Analysis to determine compliance with corporate standards and Sarbanes-Oxley regulations.

- **SOX & Compliance:** Prepared Sarbanes-Oxley audit for financial applications using CobiT//COSO model.
- **SOX & Compliance:** Analyze financial applications processes, methodologies, and systems to validate compliance to Sarbanes-Oxley sections 404 and 1102.

Client: **Sun Micro Systems - Sarbanes-Oxley**

- **SOX & Compliance:** Primary content provider for Sarbanes-Oxley initiatives with emphasis on Sarbanes-Oxley sections 302 and 404.

Client: **Pfizer Global Manufacturing, Lincoln, Nebraska**
Project Title: Information Classification
Duration: May 2004 – June 2004
Role: Project Manager
Software/Tools: Microsoft Office, MS Project

- **Compliance:** Detailed review of information objects classified under ISO 17799 standards.
- **Compliance:** Performed Gap Analysis of classified objects to determine compliance with corporate standards, 21 CFR Part 11, or Sarbanes-Oxley standards and regulations.
- **Compliance:** Prepared Remediation Analysis of objects where potential issues in implemented compliance controls were questioned.

Client: **Cendant Car Rental Group (Avis), Parsippany, NJ**
Project Title: Project Manager (Security)
Duration: January 2003 – April 2004
Role: Project Manager
Software/Tools: Microsoft Office, MS Project, RACF, Internet, and Tivoli

- **Change Management**: Reviewed the possibility of using Rational ClearQuest for tracking processing defects identified in SOX testing.
- **Security:** Security project manager for the conversion and implementation of a large mainframe based rental and reservation system. Identified and coordinated user access requirements with RACF and Database resource rules.
- **Security & Identity Management :** Assisted in review of a strategy to implement Tivoli Access and Identity Managers.
- **Security:** project manager for the conversion and implementation of a large mainframe based rental and reservation system. Identified and coordinated user access requirements with RACF and Database resource rules.
- **Security:** Reviewed web site privacy policy to for compliance with Australian and Canadian privacy laws and company PII policy and platform for privacy principles criteria.
- **Security:** Prepared project plan to remediate security and privacy issues identified in review.
- **SOX & Compliance:** Performed functional and gap analysis and created deliverables.
- **SOX & Compliance**: Developed Sarbanes-Oxley compliance and auditing program using ISO 17799, COSO, and CobiT framework.
- **SOX & Compliance** Performed Sarbanes-Oxley analysis of information technology processes comparing company policy to current practices.

Client: **Maryland Motor Vehicle Administration, Glen Burnie, MD.**
Project Title: **Information Security Analysis**
Duration: January 2002 – February 2002
Role: Security Analysis
Software/Tools: Microsoft Office, MS Project, Windows 2000, Active Directory, COM+
Description:

- **Disaster Recovery/Contingency Planning** Outlined detailed strategy to recovery state wide Moter Vehicle Licensing systems and outlined short
- **Security:** Reviewed and prepared report concerning state and federal privacy regulations relating to the issuance of drivers licenses.

- **Security:** Reviewed Windows 2000 security implementation and Network security implementation. Identifying Group Policy Options to be implemented transmission security issues such as the implementation of SSL.
- **Security:** Reviewed secure data sharing between government and a 3rd part vendors using products such as PGP and Entrust.

Client: **Bristol-Myers Squibb Pharmaceutical Research Institute, Princeton .**
Project Title: Information Security Project Manager for 21 CFR Part11
Duration: June 2001 – December 2001
Role: Project Lead
Software/Tools: Microsoft Office, UNIX and NT
Description:

- **Compliance:** Developed and document information security policies and procedures for international research institute based on 21CFR Part 11 guidelines.
- **Security**: Developed an on-boarding strategy for new employee and consultants. The strategy identified user roles and access requirements.
- **Security**: Developed formal selection criteria for Single Sign-On and PKI vendors using 21 CFR Part 11 guidelines.
- **Security:** Performed Single Sign-On vendor evaluation with emphasis strong authentication such as PKI, Tokens, and biometrics.
- requirements.

Client: **Corning, Corning N.Y.**
Project Title: Windows 2000 Security Migration Plan
Duration: December 2000 – February 2001
Role: Project Security Lead
Software/Tools: Microsoft Office, MS Windows 2000, Entrust
Description:

- **Security:** Developed MS Windows 2000 security architecture and migration plan.
- **Security:** Reviewed client's implementation of Entrust PKI and suggested for outsourcing CA.
- **Security:** Prepared policies and procedures on PKI key management.

Client: **Carlson Travel, Minneapolis, MN**
Project Title: Encryption and PKI Analysis
Duration: October 2000 – November 2000
Role: Project Lead
Software/Tools: Microsoft Office, Microsoft Project, PKI Solutions
Description:

- **Security:** Reviewed and updated corporate data privacy policies and standards.
- **Security:** Participated in re-engineering project to identify role access requirements.
- **Security:** Performed review of encryption and PKI solutions. Identify organization encryption needs and develop corporate encryption and authentication policy.

Other Accounts

Gardian Life Insurance Company: Vision 2000 Security Architecture
***Wal-Mart* Bentonville, Arkansas:** RACF Upgrade
Virginia Power and Light, Richmond, Virginia: CA-Top Secret Upgrade
Metropolitan Water District Of Southern California Contingency Plan Upgrade
Disclosure, Inc. Beheads, MD:, Disaster Recovery/Business Continuity Planning
Providian Insurance, Louisville, KY: *datatabase Reorganization*
Fidelity & Deposit Insurance Co., Baltimore, MD, *Sec*urity Analysis and Management
Metropolitan Life Insurance Company, New York City: RACF Migration
Crowley Maritime Corporation, San Francisco Ca:, RACF Implementation
Fidelity Investments, Boston Ma: Corporate Business Contingency Planning

Employment Experience

Title: **Assistant Vice President**

Employer: Citibank, New York City
Duration: New York City, September 1983 – April 1986

- Established Information Security initiative for North American Banking Group. Created and implemented policies and procedures that conformed to company and regulatory standards.

Title: Vice President, Information Security
Employer: United Jersey Banks, Princeton, New Jersey
Duration: New York City, May 1986 – April 1988

- Senior manager responsible for information security practice and compliance to regulatory standards.

Education

Bachelor of Science in Business Administration Pace University, New York City, New York

Network/Security Database Engineer

IT Audit & Information Security Engineer Arlington, VA 01/06- 06/06

Duties: IT Audit of General Support Systems and Major Applications utilizing Cobit standards and NIST guidelines. Assist in setting up the auditing environment and running simulations and activities, perform process audits on internal processes, make raw data of the audit for operational infrastructure, verify and provide accountability of all managed equipment, participate in and provide oversight of in house security tests and evaluations, conduct audits of logs from Network Intrusion Detection Systems/Host Intrusion Detection Systems, security assessment of existing and required security policies, standards and practices, conduct security audits of existing infrastructure and all delivered security artifacts (IATO, POA&M, Risk assessments). Plan and conduct integrated and technical audits, analyze data gathered to evaluate effectiveness of controls, assess threats/vulnerabilities and identify inadequate control measures. Other responsibilities: coordinate/present results to management and external auditors, collaborate with management to address control deficiencies and develop/implement improvements; facilitate monitoring practices of internal control measures employed to ensure continuous improvement, provide technical and professional guidance as it relates to information systems to audit staff, contract/external auditors and departmental management, develop automated techniques of retrieving information from business application systems and prepare audit reports to document findings and recommendations. Also provide guidance on Certification & Accreditation of General Support Systems and Major Applications utilizing NIST, FIPS 199, FIPS 201 and Presidential Directive HSPD-12.

- Senior Security Engineer Advanced Research Technology Inc. Falls Church, VA 10/04 12/05

Duties: Certification and Accreditation Manager and Continuity of Operations Coordinator. IT Audit of Major Applications and General Support Systems utilizing FISCAM audit procedures. Support several Federal agencies with IT security issues centering on IT security planning to implement network security plans. Analyze and assess their IT system security environment and provide improvement recommendations. Develop and assist in implementation of IT Security policies and Standard Operating Procedures. Implement Certification and Accreditation processes and procedures. Use standard methodologies for Certification and Accreditation processes. Follow NIST guidelines, FISMA, FIPS 199, OMB Circular A-130 Appendix III and OMB A-123 for IT systems Risk Assessment and Security Management. Analyze and develop Disaster Recovery Plans, Contingency Plans. Knowledgeable of Management, Technical and Operational Controls, Incident Response, Capability requirements, Configuration Management Plan, System Security Plan and Application Security Test and Evaluation. Assure that the Federal agencies adhere to and comply with FITSAF requirements. Also, ethical hacking to determine vulnerabilities of major applications, general support systems and remote access servers, and provide guidance on how to mitigate those findings. Other duties include business development, pre-screening of potential employees, analyzing automated tools for assistance of C&A process.

- Senior Associate Consultant 06/04 10/04 KPMG, Washington, DC

  Duties: IT Audit of client server networks (Windows 2000/2003, Novell Netware), mainframes and computer control reviews using Cobit, Sarbanes-Oxley, HIPAA, OMB A-133 and FISCAM. Developed, evaluated and reviewed system and user access controls, physical access controls, system vulnerabilities and capabilities and recommended applying operational measures to ensure system integrity and availability, Evaluated and disseminated information related to system vulnerability, determined applicability, impact, criticality and recommended corrective action procedures to management for IBM OS/390 and Microsoft Windows based platforms to ensure information systems reliability and to prevent unauthorized access to networks, systems and data. Review penetration testing, business continuity planning, information system security, system development life cycle, configuration management, database maintenance and support reviews. Also, ethical hacking, installing Windows 2003 server, Cisco VPN and inventoried in-house hardware and software.

- Cyber Security Consultant Part time /1099 06/04 10/04 Ginni Corp., Arlington, VA

  Duties: Cyber Security Consultant responsible for re-evaluating and writing security policies/plans based on Federal government standards and policies (NIST 80-18, NIST 80-26, NIST Draft 800-53) for the Department of Housing and Urban Development applications and e-commerce systems. Revaluated the department's certification and accreditation (C&A) software package to gather data, document development of system security plans, developed quantitative and qualitative risk analysis/assessments, disaster Recovery contingency plans, security policies and procedures, development for applications and servers.

- Cyber Security Engineer Contractor/1099 03/04 -05/04

  Duties: Assisted the VAs Office of Cyber and Information Security Business Assurance Program with support for complying with specific Federal Information Security Management Act (FISMA) and Office of Management and Budget (OMB) requirements regarding risk management. The effort included:
  recommendation against IT security issues; establishing policies that interrelate to business risks; and, developing practical risk assessment procedures and tools that link security to business needs.
  Assisted the Business Assurance Program in the development of a Department-wide risk management framework and associated implementation plan, establishing risk management policies and procedures; continuous monitor and evaluate risk management policy control effectiveness; developing an associated training and awareness program for all department stakeholders; assist in the conduct of risk assessments; drafting responses to requests from internal and external VA offices, and facilitating coordination and transmission of information between business line owners, OCIS programs and the Office of the Chief Information Officer pertaining to IT security related risks.
  Develop and implement a strategic Department wide risk management framework that complies with FIPS 199, FISMA, FISCAM, NIST 800-26, NIST 800-30, NIST 800-37, OMB Circular A-130, E-GOV Act of 2002.

- Lead Cyber Security Consultant responsible for creating, re-evaluating and writing security plans/policies based on Federal government standards and policies (NIST 80-18, NIST 80-26, NIST 800-37, NIST 80-44, NIST 800-53, FISMA) for the Department of Energys applications and e-commerce systems, implemented an automated certification and accreditation (C&A) software package to gather data, document development of system security plans, developed quantitative and qualitative risk analysis/assessments, disaster Recovery contingency plans, security policies and procedures, development for applications and servers in a Lotus Notes/Domino, WinNT, WinSAGA and Novell environment. Participate in IT project teams to ensure new applications and systems (Lotus Notes/Domino R6) will comply with established security policies and standards. Evaluated and recommended solutions to current or potential security threats as they relate to the computing environment. Participated in formal risk assessment reviews to determine the critical points of business exposure. Reviewed contingency plans, data integrity/validation controls, logical access

controls (Authorization/Access Controls) and recommended conducting ALE calculations of systems in the event of loss of data.

- Project Mgr/Systems Design Engineer-Contract 11/02 06/03 Milvets, Lanham, MD

  Duties: Lead technical engineer responsible for designing Local Area Networks, Wireless LANS, Security Architectures, and Cisco AVVID solutions for our various customers. Installed and configured a LAN to LAN VPN solution to establish an encrypted tunnel between a users system and the perimeter of an organizations network using L2TP protocol to set up the point to point connection. Integrated a Client to LAN VPN model so the receivers identify could be positively ensured through digital certificates and that the Diffe-Hellman exchange protocol was negotiated to process key exchange. Designed an end-to-end security architecture to encrypt data at the initiating host and decrypt at the final destination, incorporated a screened subnet to provide depth of defense, performed penetration testing for security vulnerabilities and OS hardening in an enterprise environment. Lead engineer responsible for the design and deployment of a single site Cisco AVVID model that consisted of a single Cisco Call Manager, PSTN for external calls, DSP resources for conferencing, voice mail and UM components, G711 codec for all Cisco IP phone calls and Cisco LAN switches to guarantee voice quality. Also designed a Local Area Network in a bus topology for operation in a Frame Relay environment that consists of endpoints (servers and host computers), frame relay access equipment (bridges, routers, hosts, frame relay access devices), network devices (switches, network routers, T1/E1 multiplexers) and assessed current network baseline for circuit redundancy and future scalability. Other duties included: Review RFIs/RFPs for company's technical capability and possible business development, designed company's security architecture, assessed technical personnel, equipment selection and cost analysis.

- Chief Network Engineer 7/02 11/02 MSSI, Capital Heights, MD

  Participated in the development and implementation of network security policy, ISS enabling technologies, processes and procedures into custom systems and networks (examples: Gauntlet /Sonic firewall, Intrusion Detection, vulnerability assessment, VLAN/DMZ). Utilized NetIQs security management and administration solution for real time Windows security event assessment, configuration management, host-based intrusion detection, centralized assessment and incident management, firewall analysis and reporting and Windows security administration. Update enterprise system security for virus via Symantec Norton anti-virus and system patches. Team member assigned to the business development of Voice over IP. Responsible for technical activities associated with the integration, evaluation, analysis, and support of the LAN and related hardware and software (examples: Netopia R7200 SDSL router, KVM X16 switches, OMNI View SE 4 Port Hub, COTS and Legacy software). Maintain and troubleshoot IP protocol problems and CISCO IOS problems, static NAT, DNS, routers and switches. Other duties include implementing a in Disaster Recovery plan, Change/Configuration Management Plan, Active Directory configuration, MS Exchange migration, Cluster Exchange 2000, Call Server report configuration, CA Server implementation. System administrator for Windows 2000, Tadiran Sprint PBX and Backup Exec. Also, participated in the development and implementation of a wireless web based video production network and test lab which incorporated Netware 6, Windows 2000, Exchange 5.5 and DNS.

* Systems Engineer-Temporary Contract Ended 3/02 04/02 US Resources, Falls Church, VA

  Assigued to the TIMPO/LAN infrastructure to upgrade the MEDDAC Network. Duties include: Installation and configuration of Ciscos Intrusion Detection System and the deployment of Ciscos Avvid solution in a multi-site environment. Installed Ciscos 6513 switches in the core layer for a high speed switching backbone that consisted of Gigabit Ethernet to eliminate all shared media devices within the network infrastructure utilizing Ciscos setup commands Installed and configured Ciscos Catalyst 4006 and 3500XL switches at the edge to provide 10/100 Mbps services at the distribution and access layers for redundancy to the core utilizing Ciscos IOS. Configured IP based VLAN Layer

2 architecture that incorporated the current network segments into separate VLANs. Installed SNMP, cable management rack, Cat 5E and Fiber Optic based cabling.

- Senior Systems Engineer- Company Bankrupt 1/01 09/01 Network Designs Inc., Vienna, VA Evaluated and installed different vendors Intrusion Detection Systems (Snort Sniffer, RAID, SELM and Languard) on network for invalid IP detection into environment and network compliance. Responsible for the network design of a Voice Over IP model infrastructure in a Frame Relay environment. This included various aspects of cost analysis, hardware, software, redundancy, voice messaging, and engineering of the backbone network. Thorough technical expertise and knowledge of Voice Over IP architecture, infrastructure components, signaling protocols, troubleshooting and debugging VoIP calls and other enterprise voice over data design. Utilized HP Openview Network Node Manager to manage switched layer 2 as well as routed layer 3 environments, supported heterogeneous switched networks and intelligently collected and reported network information in a remedy database, and planned for key improvements. Utilized Cisco Works 2000 for resource management of multilayer catalyst switches and access control for administering routed infrastructure in a multi service network. Installed, configured and reconfigured Cisco switches, routers and physical topologies in a LAN/WAN environment. On site technical consultant for a Madge VLAN Video Teleconferencing System. Tasks included: participating in the migration, deployment, and installation of network systems, workstations, Windows 2000 server, Snap servers, Cisco AP340 Access Point wireless hubs, Lotus Notes email conversion, office and map print applications into Windows 2000 application baseline, Jet Direct print servers and other network components. Performed data transfers, troubleshooting, resolving connectivity issues and research on fault tolerance and Recovery issues.

- Systems Engineer-Contractor - DOJ/Left for better opportunity 6/96 12/00 Northrop Grumman/Logicon, Falls Church, VA

  Utilized C2 security to prevent unauthorized access to sensitive data where multiple users had access to the same physical or network resources, used event viewer to check logs for unauthorized IP addresses and abnormalities and insured that certificate was from a trusted vendor and that certificate was valid. Point of contact for a Madge 60 VLAN Video Teleconferencing System including updating WEB page for future events relating to NMIC. Responsible for maintaining all functions of LAN/WAN (subsystems, hardware and software) for continuity and specifications and reported all problems to the NOC manager. Performed periodic updates and patches that applied to the LAN/WAN. Performed administer duties that included: adding, deleting and modifying client accounts. Set up workstations for fixed and DHCP reservations. Administrator in performing system backups and verifying the integrity of the backups on a Legato and Backup Exec System. Reviewed configurations of MED servers and all servers by SLAs in the facility. Provided after hour and weekend support via Remote Access Servers and managed assigned projects. Responsible for identifying, analyzing, installing, modifying, troubleshooting and resolving existing personal computer systems in a Unix Sun 3000, Windows NT 4.0 environment. Administrator for a Systems Manager Server (Version 1.2 SP4 Build 786) that tracks hardware, software inventory, distribute software packages and remote control diagnostics.

Telecom Engineer

- SHEARMAN & STERLING, LLP, New York, NY 2000 April, 2006
  - 1000 Attorneys/18 offices worldwide Project Manager /Senior Telecommunications Analyst.
  - Provide project management, technical assessment and analysis for the deployment of voice communications services for domestic and international offices. Manage staff, consultants and vendors for completion of various MAC projects for two Nortel 81C PBXs with Succession 3.0 software, consisting of 4,000 ports and the Octel, Call Pilot Voice Mail Systems for New York offices.

- o Reduced expenses by $300,000 annually and recovered another $250,000 in cash and credits.
- o Championed the VoIP architecture for business recovery plan utilizing both enterprise and public carriers for Cisco Call Manager Cluster with Call Unity and Nortels Communication Server 1000 with Avaya Modular Messaging on Shearman and Sterlings Sonet Ring.
- o Created strategies for billing verification and documentation from analysis of $1,300,000 in invoices from various carriers.
- o Spearheaded the networking of the Nortel PBXs, Symposium, Call Pilot and OTM through Ethernet which resulted in more efficient administration.
- o Launched the implementation of Symposium and Call Pilot for ACD and IVR of both the Support Center and Financial Services, increasing agent productivity for employee services. Documented the inventory of carrier facilities and the Voice Network through Visio and Excel for business recovery reducing down time.
- o Successfully deployed Cisco Call Manager with Cisco Call Unity for a pilot program in Rome, Italy.
- o Participated as committee member to assess Shearman & Sterling, LLP deployment and ROI for VoIP for 18 offices worldwide.
- o Negotiated rates and contracts with Verizon which significantly reduced PRI annual expenses by 55%.
- o Managed the successful deployment of Siemens Hicom PBX CBXs including Octel Voice Mail for Washington D.C., Menlo Park, and San Francisco offices.

- AOL/TIME WARNER CABLE, New York, NY 1996 2000 Telecommunications Manager
  - o Managed Siemens PBX communications for 4,000 employees servicing over one million cable subscribers and managed a staff of six for 12 offices.
  - o Reduced telecommunications expenses by $ 600,000 annually.
  - o Expanded territory to include New York 1 News, City Cable Advertising, Staten Island Cable and Bergen County Cable as awarded by Senior VP of Finance.
  - o Raised efficiencies of the voice and data cabling by accepting the management responsibilities from the IT Department.
  - o Successfully migrated 10 Nextel fleets into one increasing communications for 1000 users resulting in better communications and increased company productivity.
  - o Reduced turnover time for telephone repairs and increased client productivity.
  - o Engineered, designed, and implemented various voice networks with utilization of enterprise ATM and fiber optics eliminating carrier toll costs.
  - o Managed the operators ACD groups in Manhattan and Queens effectively reducing unnecessary staff and increased customer and employee satisfaction.
  - o Approved over $500,000 dollars annually in invoices from PBX vendors and various carriers. Successfully deployed and networked 8 Siemens Hicom CBXs in New York Offices.

- PERFORMANCE SYSTEMS INTERNATIONAL INC., New York, NY 1995 1996
  Global Internet Provider
  Senior Telecom Analyst

  - o Responsible for telecommunication operations of Siemens CBXs for North Americas six offices.

- Performed traffic studies for PsiNets national voice network and made necessary routing changes which increased sales performance and reduced operational expenses.
- Prepared and distributed ACD reports to department heads which were utilized to increase revenue.

- ASSOCIATED TELEPHONE AND DESIGN, City, ST 1992 1995
  - Channeling Partner for Nortel Networks. Manager of Installation Department, Supervised and provided technical support for a staff of eight while ensuring that contract specifications and payment schedules were met.
  - Standardized requirements for Ethernet cabling resulting in reduced operational costs. Increased productivity and reduced client installation time. Coordinated telecom installations with general contractors and architects, reducing technicians overtime.
  - Hired and negotiated with various telecommunications equipment contractors.

5.2 Project References

1. **CITY OF MEMPHIS**
   125 N. MAIN STREET, SUITE # 528
   MEMPHIS, TN
   Contact Person: CHARLES ELLIOTT
   Tel # 901-576-7050
   Email: CHARLES.ELLIOTT@MEMPHISTN.GOV

2. **CITIGROUP**
   3800 CITIGROUP DRIVE
   TAMPA, FL-33610
   Contact Person: Arup Gosh, Vice President
   Ph: (813)-604-2092
   Email: arup.g.gosh@citigroup.com

3. **FED EX**
   1900 Summit tower blvd.
   MEMPHIS, TN
   Contact Person: Mike Ike
   Ph: (901)-218-6233
   Email: mikeike@gmail.com

4. **Lincoln National Life Insurance**
   1300 Clinton Street
   Ft. Wayne, IN – 46802
   Contact Person: Mr. Jim Wright, Project Manager
   Ph # (219) 455- 3352

5. **MCI/AVANTEL**
   Garden of the Gods Road
   Colorado Springs, CO
   Contact Person: Mr. Unnikrishnan Kumar, Project Lead
   Ph # (719) 535-6733

6. **Alternative Resources Corp.**

8310 Capital of Texas Hwy. N, Suite # 410
Austin, TX 78731
Contact Person: Mr. Rusty Johnson, General Manager
Tel # (512)-343-1700
Fax # (512)-343-7228, Email: rusty_Johnson@alrc.com

6.0 SECTION 6: APPENDIX

6.1 Disaster-Recovery Plan Data Gathering Template

SAMPLE TEMPLATE

Disaster-Recovery Plan

For: _____

Location: _____

Version 1.0, Date: _____ _____
Copy Number

CONFIDENTIAL
This disaster recovery plan is confidential and is not to be distributed to anyone beyond the individuals indicated in the stated distribution policy within. Should any external individual or entity request any copies of this plan, the request should be referred to the Disaster Recovery Office.

IN CASE OF EMERGENCY

IMMEDIATELY NOTIFY ANY OF THE KEY EMERGENCY CONTACTS LISTED BELOW:

Contact	Office Number	Home Phone
Security Desk		
In the event that none of the above key contacts are available, call		

MANAGEMENT APPROVAL

This Disaster Recovery Plan, Version 1.0, has been approved by the undersigned:

_____ DATE: _____

_____ DATE: _____

_____ DATE: _____

_____ DATE: _____

Disaster recovery Planner

SAMPLE TABLE OF CONTENTS

MANAGEMENT APPROVAL

1. DISASTER RECOVERY PLAN OVERVIEW

1.1 POLICY STATEMENT

1.2 SCOPE OF PLAN

1.3 ASSUMPTIONS

1.4 BUSINESS IMPACT ANALYSIS

1.5 CRITICAL BUSINESS FUNCTIONS

1.6 RECOVERY STRATEGIES

1.7 PHASES OF RESPONSE

1.8 RECOVERY ORGANIZATION

1.9 ROLES AND RESPONSIBILITIES

1.10 DISTRIBUTION POLICY

2. EMERGENCY MOBILIZATION

2.1 INTRODUCTION

2.2 EMERGENCY OPERATIONS CENTER

2.3 EMERGENCY MANAGEMENT TEAM

2.4 EMERGENCY OPERATION CENTER PREPARATION

2.6 EMERGENCY MANAGEMENT TEAM NOTIFICATION TREE

3. TEAM ACTION PLANS

3.1 EMERGENCY MANAGEMENT TEAM ACTION PLAN

3.2 Mission Critical System - Template (1 per system)

4. TESTING AND MAINTENANCE

4.1 MAINTENANCE SCHEDULE

4.2 EVENT TRIGGERED REVIEWS

4.3 TESTING

4.4 DISASTER RECOVERY PLAN UPDATES AND DISTRIBUTION

5. APPENDIX

Facilities Emergency Procedures

Master Employee Listing

Damage Assessment Checklist

Directions to Emergency Operations Centers

Approved Press Release

Recovery Status Report

Testing and Maintenance Schedules

Test Results

Test Guides

Maintenance Log

Maintenance Request

Reciprocal Agreements

Document Control Sheet

Dependency Roll-Up

Vital Record Summary

Corporate Risk Management Policy

1. OVERVIEW

1.1 POLICY STATEMENT

1.2 SCOPE OF PLAN

1.3 ASSUMPTIONS

1.4 BUSINESS IMPACT ANALYSIS

1.5 CRITICAL BUSINESS FUNCTIONS

CRITICAL BUSINESS SYSTEMS/FUNCTIONS	RECOVERY TIME OBJECTIVE

Note: All recovery time objectives, other than immediate, reflect business days or weeks.

1.6 RECOVERY STRATEGIES

I. TRANSFER OF WORK	
Advantages	***Disadvantages***
• Can be done relatively quickly • Works regardless of damage severity • Requires little initial set up cost	• Places burden on recipient business unit • Lack of staff familiarity may impact work quality and customer satisfaction
II. IN HOUSE RECOVERY	
Advantages	***Disadvantages***
• Minimizes impact on other business units • Continuity of staff has positive effect on quality and job performance •	• Typically takes more time to implement • Recovery may not be practical with some severe disasters which affect availability of staff and/or recovery locations •
III. AT HOME	
Advantages	***Disadvantages***
• Can be done relatively quickly	• Lack of staff ability to interact may impact work

• Works regardless of damage severity • Requires little initial set up cost	quality • Lack of equipment and remote accounts may limit response

1.7 PHASES OF RESPONSE

1.8 RECOVERY ORGANIZATION

1.9 ROLES AND RESPONSIBILITIES

1.10 DISTRIBUTION POLICY

2. EMERGENCY MOBILIZATION

2.1 INTRODUCTION

This chapter covers the process by which the plan is activated. As explained in chapter one, a business disruption has three distinct phases: Emergency, Recovery, and Restoration.

2.2 EMERGENCY OPERATIONS CENTER

The emergency operations center (EOC) is the focal point of communication and coordination for resources during a business disruption.

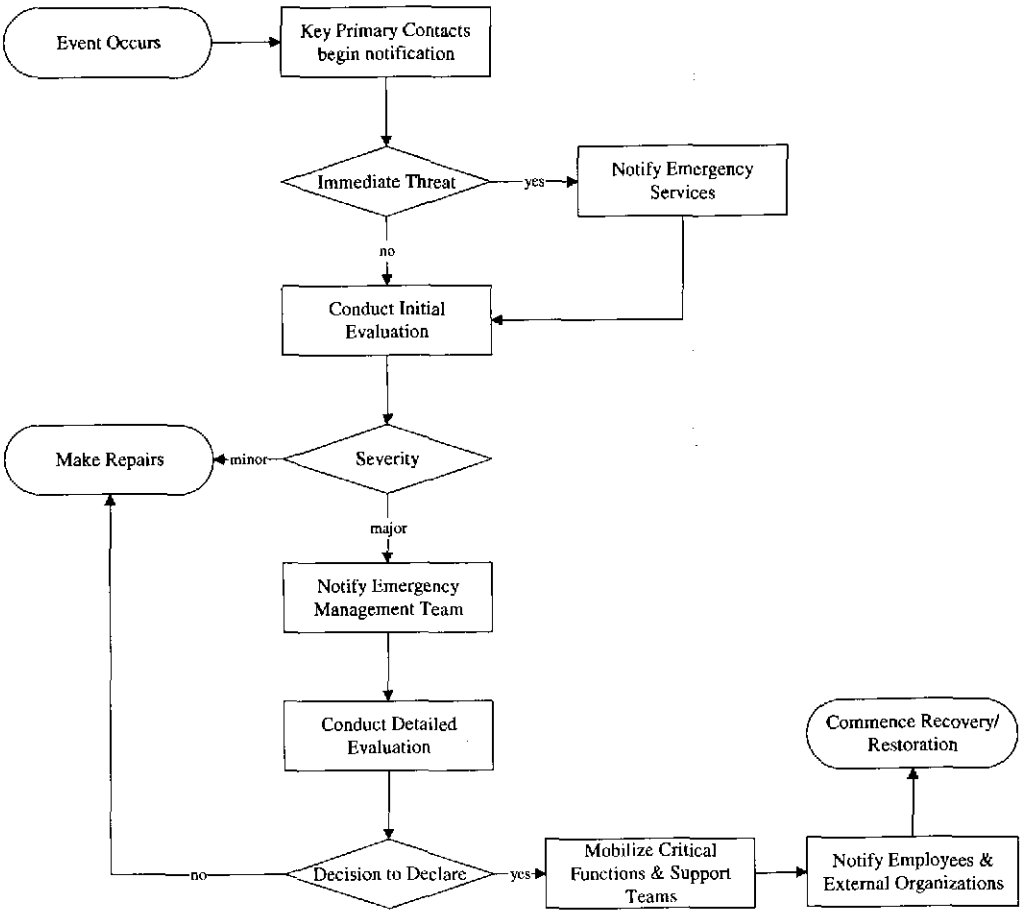
Two sites have been selected as possible EOC locations. The preferred site has been designated as the primary EOC and is located at:

2.3 EMERGENCY MANAGEMENT TEAM

2.4 EMERGENCY OPERATION CENTER PREPARATION

2.5 PROCEDURES

The chart below outlines the steps taken during notification and mobilization. The procedures that follow indicate who is responsible for the specific actions.



	PROCEDURES	WHO
1.	**ACTIVATE EMERGENCY PROCEDURES/NOTIFY SITE EXECUTIVE** Upon discovery of an emergency, immediately activate emergency procedures in accordance with the property manager's policy for life safety and damage mitigation (in Appendix). The Primary Contacts will notify "YOUR DEPARTMENT" Executive, or alternate, and provide the status of the facility/event.	
5.	**NOTIFY KEY CONTACTS** In addition, the following key individuals should be contacted	
11.	**NOTIFY EMPLOYEES** All employees and staff not previously notified will be contacted by the Emergency Management Team Members per the Notification Tree (see 2.6) and provided with any pertinent instructions to follow.	Team Leaders

2.6 EMERGENCY MANAGEMENT TEAM NOTIFICATION TREE

Notifier	EMT Role	EMT Member	Numbers	Remarks
	EMT Leader			

H = home W = work P = pager C = cellular S = satellite
F = fax

3. TEAM ACTION PLANS

This section contains specific procedures for the established Disaster recovery Teams to follow during the various stages of a disaster.

3.1 EMERGENCY MANAGEMENT TEAM ACTION PLAN

Emergency Phase

	PROCEDURE	WHO
1.	**REVIEW DAMAGE SURVEY AND DETERMINE NEXT STEPS** Team Leader reviews available information and consults with key team members to determine if declaration will be made. ***ONLY THE TEAM LEADER (OR ALTERNATE) CAN MAKE A DECLARATION.***	

Recovery Phase

	PROCEDURE	WHO
1.	**MONITOR RECOVERY OPERATIONS OF CRITICAL FUNCTIONS** Once the immediate effects of the disaster have been addressed, the Emergency Management Team's primary responsibility will be to monitor individual team plan implementation for: * Ensuring adequate resource distribution to meet business needs. * Coordinating activities with support areas. * Reviewing/approving deviations from established plans.	

Restoration Phase

	PROCEDURE	WHO
1.	**COORDINATE WITH SERVICE PROVIDERS AND THE "YOUR DEPARTMENT" STAFF FOR MIGRATION OF WORK TO THE RESTORED (OR NEW) FACILITY** The Emergency Management Team will oversee the transition of work back to EPW. Working with the functional teams, the EMT should ensure that: • Appropriate equipment is up and operational. • System connections have been reestablished. • Business contacts have been informed. • Appropriate vendors have been notified.	

RESOURCE ITEMS

Item	Contact/Location/Phone
Space • Work spaces (staff) including ability for working shifts/overtime.	Work from home

3.2 Mission Critical System - Template (1 per system)

MISSION

CRITICAL BUSINESS PROCESSES	RECOVERY TIME OBJECTIVE

Disaster Notification	Immediate
Disaster Response	Immediate

TEAM MEMBERS

	Name	Phone Numbers	Remarks
Team Leader			
Alternate			
Member			
Member			

H = Home; W = Work; C = Cell; P = Pager; S = satellite

TEAM PROCEDURES

Emergency Phase

	PROCEDURE REVIEW & USE/MODIFY BELOW	WHO
1.	**COORDINATE WITH EMT TO DETERMINE MOST LIKELY OUTAGE PERIOD.** Team leader will be contacted by "YOUR DEPARTMENT" executive and will report to the emergency operation center for information on the estimated duration of the outage and any special concerns that may affect recovery operations.	

Recovery Phase

	PROCEDURE	WHO
1.	**COORDINATE TRANSFER OF WORK** If transfer of work is necessary, contact Corporate Security.	

Restoration Phase

	PROCEDURE	WHO
1.	**COORDINATE TRANSFER OF WORK BACK TO PERMANENT "YOUR DEPARTMENT" SITE** Based on the status of the restoration, determine when associates and work functions can return to the permanent site. If necessary return may be phased to allow a gradual return to normal. Coordinate with recovery sites for schedule of work transfer. Inform staff members of scheduled move. Notify vendors	

	PROCEDURE	WHO
	for mail and other services for resumption of normal operations.	

RESOURCE ITEMS

Item	Contact/Location/Phone
Space • Work spaces (staff) including ability for working shifts/overtime.	Work from home

H = Home; W = Work; C = Cell; P = Pager; S = satellite

4. TESTING AND MAINTENANCE

4.1 MAINTENANCE SCHEDULE

4.2 EVENT TRIGGERED REVIEWS

The following table includes many events that may necessitate a maintenance review. While this list is extensive, there may be additional conditions not listed that could also justify a review:

Situation	**Actions Taken**
Is there a change to a current critical function?	Review all information associated with the function (RTO, processes, procedures, etc.) and revise as needed

4.3 TESTING

4.4 DISASTER RECOVERY PLAN UPDATES AND DISTRIBUTION

5. APPENDIX

CONTENTS

Facilities Emergency Procedures	Tab A
Master Employee Listing	Tab B
Damage Assessment Checklist	Tab C
Directions to Emergency Operations Centers	Tab D
Approved Press Release	Tab E

DAMAGE ASSESSMENT CHECKLIST - SAMPLE

Structure

Nature of Disruption:_____

Type of Damage: _____

Rate Severity: ☐ None ☐ Slight ☐ Bad ☐ Total Loss

Rate Duration: ☐ 12 hrs ☐ 24 hrs ☐ 2 Days ☐ 1 Week ☐ 2 Weeks ☐ Longer

Input received from:_____

Electrical

Nature of Disruption:_____

Type of Damage: _____

Rate Severity: ☐ None ☐ Slight ☐ Bad ☐ Total Loss

Rate Duration: ☐ 12 hrs ☐ 24 hrs ☐ 2 Days ☐ 1 Week ☐ 2 Weeks ☐ Longer

Input received from:_____

Communications

Nature of Disruption:_____

Type of Damage: _____

Rate Severity: ☐ None ☐ Slight ☐ Bad ☐ Total Loss

Rate Duration: ☐ 12 hrs ☐ 24 hrs ☐ 2 Days ☐ 1 Week ☐ 2 Weeks ☐ Longer

Input received from:_____

Data Center

Nature of Disruption:_____

Type of Damage: _____

Rate Severity: ☐ None ☐ Slight ☐ Bad ☐ Total Loss

Rate Duration: ☐ 12 hrs ☐ 24 hrs ☐ 2 Days ☐ 1 Week ☐ 2 Weeks ☐ Longer

Input received from:_____

Heating/Ventilating/Air Conditioning

Nature of Disruption:_____

Type of Damage: _____

Rate Severity: ☐ None ☐ Slight ☐ Bad ☐ Total Loss

Rate Duration: ☐ 12 hrs ☐ 24 hrs ☐ 2 Days ☐ 1 Week ☐ 2 Weeks ☐ Longer

Input received from:_____

Environmental

Nature of Disruption:_____

Type of Damage: _____

Rate Severity: ☐ None ☐ Slight ☐ Bad ☐ Total Loss

Rate Duration: ☐ 12 hrs ☐ 24 hrs ☐ 2 Days ☐ 1 Week ☐ 2 Weeks ☐ Longer

Input received from:_____

General Offices

Nature of Disruption:_____

Type of Damage: _____

Rate Severity: ☐ None ☐ Slight ☐ Bad ☐ Total Loss

Rate Duration: ☐ 12 hrs ☐ 24 hrs ☐ 2 Days ☐ 1 Week ☐ 2 Weeks ☐ Longer

Input received from:_____

RECOVERY STATUS REPORT

The Recovery Status Report is completed by each recovery team member to document his or her activities. This checkpoint report should be given to the Team Leader. All of the requested information is to be completed for each to enable monitoring the progress of the recovery. The Emergency Management Team uses this information to provide briefings to senior management and to analyze the recovery once normal operations are restored.

Name:_____ Team Name:_____

Title:_____ Date/Time:_____

Subject/Location:

_____

Findings/Observations:

_____

Recommendations:

_____

MAINTENANCE LOG

The chart below will be used to record when maintenance is performed on the various sections and Team Action Plans that make up this Disaster recovery Plan document.

Date	New Version	Description of Activity	Next Review

PRESS RELEASE

Press Releases / Media Statements to be used at time of disaster or serious disruption:

"A (fire, power outage, etc.) has temporarily disrupted operations at "YOUR COMPANY" located in _____. (No, some, exact count) employees in the facility at the time of the event were injured (and were taken to _____ for treatment.)

6.2 GIT Financial Statements

NOTE: See Attached

APPENDIX 18

18. NSE Original Analysis

Appedix Details begin on Next Page

Sub-Saharan Africa: Definitional Mission to Nigeria and Ghana Stock Exchange

Table of Contents

Executive Summary....5

NSE Disaster Recovery Plan and Systems BackUp....8

Preface: Nigeria Stock Exchange....8

B. Project Description....10
- About the Grantee and....10
- Partner Organizations....10
- Introduction to Data Centers Backup and Disaster Recovery....11
- Technology Considerations....12
- Operations and IT Findings at NSE, CSCS and SEC....13
- Operating Environment at NSE and CSCS....20

C. Developmental Impact....21

D. Implementation Financing....21

E. U.S. Export Potential....21

F. Foreign Competition....22

G. Impact on the Environment....23

H. Impact on U.S. Labor....23

I. Qualifications Required by the TA Contractors....23

Grantee's Request....25

J. Justification....25

K. Terms of Reference and Budget....26
- Aim of Terms of Reference....26
- Tasks and Scope of Work....26
- Budget for Technical Assistance....34

M. Recommendation....34

Budget for Nigeria Disaster Recovery Technical Assistance to NSE....35

GSE Automated Trading and SEC Surveillance Systems....36

Preface: Ghana Stock Exchange....36

B. Project Description....37
- Introduction....37
- About the Grantee....38
- Background of the Project....38
- Functional & Technical Specifications....39

C. Developmental Impact....42

Sub-Saharan Africa: Definitional Mission to Nigeria and Ghana Stock Exchange

D. Project Sponsor's Commitment 43
E. Implementation Financing 43
F. U.S. Export Potential 43
G. Foreign Competition 43
H. Impact on the Environment 44
I. Impact on U.S. Labor 44
J. Qualifications Required by the FS Contractor 44
Grantee's Request 45
K. Justification 45
L. Terms of Reference and Budget 46
Aim of the Terms of Reference 46
Tasks and Scope of Work 46
Outline of the Terms of Reference 46
M. Recommendation 48
Budget for Ghana Technical Assistance to GSE and SEC 49
Technical Assistance on Cross-Border Listing Between NSE and GSE 50
Preface: Integrating Capital Markets 50
B. Project Description 51
About the Grantee 51
Background 53
C. Development Impact 53
D. Project Sponsor Commitment 53
E. Implementation Financing 54
F. US Export Potential 54
G. Foreign Competition 54
H. Impact on the Environment 54
I. Impact on US Labor 54
J. Qualifications Required by the FS Contractor 54
K. Justification 56
L. Terms of Reference and Budget 56
Aims of the Terms of Reference 56
Scope of Work 57
Outline of the Terms of Reference 58
Budget for Technical Assistance 61

Sub-Saharan Africa: Definitional Mission to Nigeria and Ghana Stock Exchange

Budget for Cooperation Among West African Stock Exchanges 62
Other Projects and Considerations – Not Recommended..... 64
Nigeria..... 64
Ghana..... 66
Contacts Consulted During DM..... 68
Washington, D.C. 68
Nigeria 68
Ghana..... 74
Annex I: Nigeria Capital Market Diagram 78
Annex I: Trade Transaction Flow – Nigeria..... 79
Annex I: Trade and Settlement Transaction Flow – Ghana 80

Sub-Saharan Africa: Definitional Mission to Nigeria and Ghana Stock Exchange

Acronyms

APDF	Africa Project development Facility
BRVM	Bourse Regionale des Valeurs Mobilieres
CBG	Bank of Ghana . (Central Bank of Ghana)
CFA	Unit of West African Currency
CSCS	Central Securities Clearing System Ltd, Nigeria
CSD	Central Securities Depository of Ghana
Depository	Central Securities Depository of Ghana
DM	Definitional Mission
DR	Disaster Recovery
ECOWAS	The Economic Community Of West African States
e-IPO	Electronic Initial Public Offering
EMC	EMC Corporation Inc.
FINSSP	Financial Sector Strategic Plan of the Government of Ghana
GB	Gigabits
GSE	The Ghana Stock Exchange
ICT	Information and Communications Technology
IDA	International Development Association of the World Bank Group
IPO	Initial Public Offering
IT	Information Technology
LAN	Local Area Network
NEPA	National Power Authority of Nigeria
NITEL	Nigerian Telecommunications Authority
NSE	The Nigerian Stock Exchange
PFA	Pension Fund Administrators
RAM	Random Access Memory
SEC	The Securities and Exchange Commission of Nigeria
SECG	The Securities and Exchange Commission, Ghana
SME	Small and Medium Enterprise
SQL	Standard Query Language
SSNIT	Social Security and National Insurance Trust
STP	Straight though processing
T-bills	Treasury Bills
TCP/IP	Transmission Control Protocol/Internet Protocol used to connect hosts on the Internet
TGF	Trade Guarantee Fund
US$	United States Dollar
USAID	United States Agency for International Development
USTDA	United States Trade and Development Agency
VSAT	Very small aperture terminal, an earthbound station used in satellite communications of data voice and video signals, excluding broadcast television
WAMI	West African Monetary Institute
WAMZ	West African Monetary Zone
WAN	Wide Area Network
WB	World Bank

Sub-Saharan Africa: Definitional Mission to Nigeria and Ghana Stock Exchange

A. Executive Summary

In November 2005, Computer Frontiers Inc. conducted a Definitional Mission (DM) on behalf of the United States Trade and Development Agency (USTDA) to Nigeria and Ghana to review the Information and Communications Technology (ICT) capacity of the Stock Exchange in Nigeria and Ghana respectively.

The misson examined the request of the Nigerian Stock Exchange (NSE) that USTDA consider providing assistance for the development of an emergency response system that would include procurement of back-up software, hardware, and plans for the establishment of a secure, secondary location in case of an emergency at NSE.

In Ghana the mission examined the request of the Ghana Stock Exchange (GSE) for assistance to modernize its IT infrastructure, to include the implementation of an automated trading system. The DM also reviewed the ICT requirements of the Securities and Exchange Commission (SECG).

In addition the DM discussed the need for the cross-border listing of securities among West African stock exchanges. The DM team discussed cross-border listing issues with the stock exchanges as well as the West African Monetary Institute (WAMI).

Currently U.S. equipment software is widely used by the exchanges. To maintain the continued use and to take advantage of additional opportunities for the export of U.S. goods and services to the area, the DM recommends two projects for USTDA consideration:

1. Technical assistance to NSE to develop a disaster recovery plan and systems back-up.

2. Technical assistance to GSE and SECG to define their technology needs and to access a recently approved IDA credit.

3. Technical assistance to the West West African Monetary Institute to conduct a study on constraints to cross-border securities listings among two West African stock exchanges - the Nigerian Stock Exchange and the Ghana Stock Exchange.

Disaster Recovery Plan and Emergency *Backup System for the Nigerian Stock* Exchange

The Nigeria Stock Exchange and the Central Securities Clearing System (CSCS) are located in the same 24-story building in the middle of the congested financial center in Lagos. NSE and CSCS currently occupy floors 2, 3, 8 and 23. The main disaster threatening the operations of the Nigerian Stock Exchange at this time is the threat of fire, either electrical or accidentally started. The office spaces are overcrowded and outside help cannot be relied upon due to the location of the building, lack of fire hydrants or running water in the neighboring area, the height of the building, and the gridlock traf-

Sub-Saharan Africa: Definitional Mission to Nigeria and Ghana Stock Exchange

fic pattern in the district making it hard to access. Other factors weighing negatively are the exit unfriendly building design as well as the lack of experience in extinguishing high-rise building fires by the Lagos Fire Department. Despite the solid thick cement walls and foundation, the building is a potential firetrap.

The secondary objective of the redundancy is to provide a mechanism for continuous trading and support of the exchange in case of failure of the main building or main equipment. Business continuation of processes and services is critical for an expanding exchange where volume transactions are doubling each year, capitalization is growing at 30% annually, and the expected new listings and new money coming to the capital market place is expected to double in the next three years.

We estimate the total project cost for establishing a back-up facility, at an alternate site, at about US$2 million, of which there will be about US$800,000 worth of equipment, software and services potential for US suppliers.

In addition to providing valuable technical service and solutions to NSE to facilitate its reliability, availability and future growth, we believe that USTDA's support would open opportunities for U.S. companies in the $ 1 to 2 million range over one to two years, and would help displace competition from South African and European companies.

The recommended consultancy for the DR is estimated to cost US$236,410.

Technical Assistance to the Ghana Stock Exchange and Securities & Exchange Commission

The Ghana Stock Exchange requests technical assistance (a) to define a project to automate its manual trading, clearance, settlement and surveillance systems (b) to help establish connectivity between GSE and CSD and SEC systems and (c) to help it access an IDA credit, which includes a component for GSE automation. GSE was not able to take advantage of peviously approved IDA funding for automation for multiple reasons, some outside its control. If GSE is not able to access IDA funding on this occasion, it plans to lease a software package from Millenium of Sri Lanka.

The same IDA credit allocates US$6.7 million to strengthen the The Securities and Exchange Commission of Ghana. SECG requests USTDA assistance to help define its IT requirements for its surveillence function as well as to interface with the GSE and Cental depository.

The Government of Ghana is commited to financial sector reform. Key elements of the strategy are to strengthen the SEC and upgrade the technology at GSE for trading securities. In addition there will be IT connectivity to market participants, and in the course of time, to other exchanges in West Africa. If U.S. consultants get involved in this process now, and develop an IT strategy for SEC and GSE, it is likely that they would look to US suppliers of technology and hardware. We believe that USTDA's support would open opportunities

Sub-Saharan Africa: Definitional Mission to Nigeria and Ghana Stock Exchange

for U.S. companies of about US$ 1-2 million over a two to three year period. It would also help the US to establish a presence in a growing sector, which USAID has supported.

At this time, GSE and SEC have made no commitment for consultants, software or hardware, though GSE is leaning towards the Sri Lankan Millenium software which is in use by the Depository and the Mauritius Stock Exchange.

We propose that USTDA commit to provide consultancy services to GSE and SECG of up to US$57,660. A small commitment now, will establish a US presence and may help US consultants to acces funding from the IDA Credit for additional services related to Ghana's capital markets.

Cooperation among West African Stock Exchanges

Plans to integrate West Africa's stock exchanges have been under discussion for sometime as it is felt that pooling the resources of these small capital markets could boost their ability to mobilize local and international capital for development. Pending integration, strategic alliances among them, and with larger hubs, could significantly reduce the cost of cross-border investment activity.

The West African Monetary Institute (WAMI) was established and has been tasked by the countries in the West African Monetary Zone (WAMZ) to nurture the WAMZ countries into a monetary union. Pending monetary union, now targeted for 2009, WAMI considers that the time is appropriate to stimulate cross-border investments.

As a first step it has proposed a study of the policy, regulatory and tax frameworks that are constraints to cross-border listings among the Ghana Stock Exchange and the Nigerian Stock Exchange. The study will also recommend steps required to harmonize the listing requirements of each exchange, and recommend uniform accounting and reporting standards to eliminate duplication of efforts and costs by listed companies. A recent secondary listing on the Johannesburg Stock Exchange by a Nigerian company, OandO Plc. cost approximately US$2 million.

The DM proposes that USTDA provide funding of up to US$199,540 for this study.

NSE Disaster Recovery and Plan and Systems Back-Up

NSE Disaster Recovery Plan and Systems BackUp

Profiles Nigeria Stock Exchange

The NSE (formerly the Lagos Stock Exchange) was established in 1960 with 19 securities listed for trading. Today NSE lists 276 securities, made up of 17 Government Stocks, 50 Industrial Loans (Debentures / Preference) Stocks and 209 equities of companies, with a total market capitalization of N2.23 trillion (US$15.7 billion equivalent). The listed companies represent a cross section of the economy – from agriculture to petroleum marketing, banks, managed funds, food, beverage and tobacco, industrial products and conglomerates.

The NSE headquarters are in Lagos with six trading floors and branches in Kaduna, Port Harcourt, Kano, Onishta and Ibadan.

The NSE derives its income from three main sources: an annual quotation levy, application and processing fees, and a fee levied on each equity (sell) transaction. The Exchange is self sufficient and profitable, and operates at a surplus. Net income in 2004 was US$1 million equivalent on revenues of US$18.5 million equivalent.

The NSE is well developed in terms of number of listings, branch network, technology, settlement and custodial systems. It has a tested network of stockbrokerage firms, issuing houses, registrars, corporate law firms and over 50 auditors and reporting accountants (several with international affiliations). Audit reports are reviewed by both SECN and NSE. The quality of the audits has improved over time.

Foreign Investments

Following the abrogation of the Exchange Control Act of 1962 and the Nigerian Enterprise Promotion Act of 1989, foreigners can now participate in the Nigerian market both as operators and investors. There are now no limits to the percentage of foreign holdings in any registered Nigerian company. Tax rates for both residents and non-residents are 10% on dividends and capital gains respectively.

Company Listings

It is difficult to estimate the potential number of companies capable of listing, but it is safe to conclude that the number of listings is small, relative to the size of the economy. Factors inhibiting listings include disclosure requirements and scrutiny, offshore profit taking, the culture of wanting to keep for yourself what you have built-up, the ability of some significant indigenous enterprises to raise equity from family related enterprises, access to local and international credit on favorable terms. While some enterprises have shied away for many of these reasons, the high cost of listing, estimated at between 5-7% of an issue, and the recurring costs of maintaining a listing appear to impact on their not accessing the market.

Government policy, action or inaction has led to spurts or stagnation in the number of listings. The indigenization program in the 1980s, which required majority Nigerian ownership of companies, resulted in a dramatic increase in listings by foreign-owned

NSE Disaster Recovery and Plan and Systems Back-Up

companies. High interest rates in the mid-1990s, led to a second set of listings by companies seeking cheaper capital. The Government's privatization program was substantially stalled in 2004, and the listings anticipated from privatization did not materialize. In the few privatizations that matured, like that of Nigerian Airlines, the stock in the new airline Virgin Nigeria was sold privately to core investors. However, this was offset by seven new equities listed in 2004, five of which were banks, seeking to meet the Central Bank of Nigeria's requirement that all banks in Nigeria maintain an equity base of N25billion (approx. $195 million).

Two on-going Government programs are likely to spur the demand for listed securities – pension reform, and privatization of the National Electric Power Authority (NEPA), the Nigerian Telecommunications Authority (NITEL), and the refineries.

Reform of the Pension Sector is almost complete. Thirty-seven private sector Pension Fund Administrators (PFA) will have responsibility for investing pension funds. While no more than 20% of pension monies can be invested in equities, the PFAs will seek corporate and government bonds listed on NSE.

The privatization of NEPA, NITEL, and the refineries will also need substantial local and foreign capital. NEPA has been dismantled into regional generating and distribution hubs. Power Holding Company of Nigeria Plc. holds its assets, and intentions are to securitize each hub and seek fresh non-government capital for modernization and expansion. But privatized power companies and NITEL are unlikely to come to market for at least two years. Discussions on the refineries, however, are more advanced.

The Securities and Exchange Commission of Nigeria (SECN) and the NSE have active programs to promote listings as well as share ownership. NSE has an energetic program called the Emerging Markets Program to encourage small to medium scale enterprises to list. To date, sixteen companies are listed with a total capitalization of US$3.9 million equivalent. The paid-in share capital of these companies ranges between US$150,000 – US$200,000 equivalent. NSE has also undertaken overseas promotions, more recently to the US, to showcase the exchange as well as stimulate the interest of non-resident Nigerians to invest through NSE.

Trading System

NSE has operated a screen based automated trading system (ATS) since 1999, with dealers trading through a network of computers, remotely or from the exchange floor. The United Nations Development Program supported the cost of automation and staff development.

Clearing, settlement and delivery of transactions are done electronically by the Central Securities Clearing System (CSCS), a subsidiary of NSE. CSCS also offers custodian services. Settlement is T+3 meaning the Delivery vs Payment is achieved as stock and funds exchange between buyers and sellers on the fourth business day. Market prices and quotes, along with an All Share Index are published

NSE Disaster Recovery and Plan and Systems Back-Up

daily in the NSE's Daily Official List, Reuters & local newspapers.

B. Project Description

	Project Summary Information
Host Country	Nigeria
Project Name	Disaster Recovery
Sector	Financial
Region	Sub-Saharan Africa
Project Location	Lagos, Nigeria
Project Cost	$ 2 Million
U.S. Exports	$ 0.8 Million
Project Sponsor	
Grantee	NSE

About the Grantee and Partner Institutions

The Nigerian Stock Exchange would be the grantee.

Nigerian Stock Exchange (NSE) – The NSE is ranked second among Sub-Saharan exchanges in terms of market capitalization. A Council of 12 members drawn from NSE stakeholders and leading businesspersons governs NSE. The NSE is well managed and has skilled and competent staff. The Director General, Mrs. Ndi Okereke-Onyiuke, provides strong and consistent leadership. Most senior staff members have had significant overseas exposure. In 2004 NSE employed 127 persons, of whom 74 were in executive grades.

Central Securities Clearing System (CSCS) -- The CSCS was incorporated as a subsidiary of the Nigerian Stock Exchange (NSE) on July 29 1992 and was licensed by the Securities and Exchange Commission as a Central Depository Clearing and Settlement Agency. The CSCS commenced operations on April 14 1997. Today, it is an independent institution of which NSE holds 30.4%, Settlement banks hold 47.7% and other Institutional investors hold the remaining 22%. The CSCS operates a computerized depository, clearing, settlement and delivery system for transactions in shares listed on the Nigerian Stock Exchange. It began with a T+5 days settlement cycle which on March 1, 2000 was reduced to T+3.

The primary function of the CSCS is the clearing and settlement of transactions on the Nigerian Stock Exchange. They also serve as the central depository for share certificates of quoted companies on NSE, as well as a sub-registry for all quoted securities. CSCS estimates they hold 50% of all shares listed with the remainder being held by investors who have not traded their shares yet. The CSCS also provides custodian services in conjunction with the custodian members for local and foreign investments.

To facilitate these functions, the CSCS issues Central Securities Identification Numbers to Stockbrokers and Investors. These are unique numbers stored in a large database and allow for proper logging, tracking and security of transactions. This is valuable data linking all transactions to their originator with all trading details of account number, number of shares, date of transaction, amounts transacted, etc. Securing this database is of utmost importance to the operations of NSE and CSCS as without it no trading can occur.

NSE Disaster Recovery and Plan and Systems Back-Up

Securities and Exchange Commission (SEC) -- The SEC is the apex regulatory body for the Nigerian capital market. The 'Investments and Securities Act No 45' of 1999 is expected to promote a more efficient and virile capital market which would be critical in meeting the nation's economic and development aspirations. SEC protects investors' interests and thereby enhances their confidence in the capital market. SEC also ensures orderly and equitable dealing in securities business and promotes capital market growth and development. They are headquartered in Abuja with three satellite offices including one in Lagos.

Introduction to Data Centers Backup and Disaster Recovery

Detailed research of the existing IT environment and its requirements coupled with the needs for redundancy and scalability will ultimately determine the most appropriate DR or Backup solution and its implementation. To gain a better understanding, the DM conducted a preliminary look at the following areas currently at NSE and CSCS. The findings of the DM research team across these areas are outlined in the section on "Operations and IT Findings in NSE, CSCS and SEC."

- *Application / System Design* – includes application data flow, network diagram, inventory of hardware, security controls, list of applications with 3rd party vendor remote access or external connectivity
- *Development* – includes application tools, change control process, Quality Assurance process, development infrastructure
- *End-to-end Authentication* - Security/authentication information includes user account and password management
- *Database Authentication* - Security/authentication information includes user account and password management
- *End-to-end Authorization* - Authorization methods currently in place, process in which users are provided permission, access levels, etc.
- *Operating Environment* - Operating procedures which ensure all systems are fully patched and kept up-to-date
- *Support* - operational model for supporting the application's databases/servers, and access control for enterprise and production systems
- *Networking* - Network management and protocol descriptions
- *Firewalls* - Production and Enterprise Firewall management
- *Monitoring/Logging* - how security monitoring (including logging) is performed to ensure secure configuration and protection against system misuse
- *Business Continuity* - Disaster Recovery/Business Resumption strategy
- *Backups* - controls/procedures currently in place for back up

NSE Disaster Recovery and Plan and Systems Back-Up

- *Physical Security* - security procedures at Data centers and main locations

The research of requirements for future DR site or need for redundancy has to answer the following questions:

1) *Purpose for the redundancy* – why is it needed, what is to be gained or protected, what is the business justification. This will help shape the location, scale and security requirements

2) *Service Level Agreement SLA Expectations* – how fast is the failover required, how current is the data expected to be, what is the expected performance of the backup/DR site, what are the expectations for the support team, uptime, availability and reliability expectations of the new site

3) *Networking, Connectivity and Circuits* – what is the networking requirement and options, are data transfers done over the network, over internet or over leased private lines, what is the available vs desired throughput and method, can the circuits handle the data replication traffic

4) *Power Consumption* – what are the requirements for use of power and the available vs desired sources, are there UPS or building generator facilities available to supply building power

5) *Cooling Capabilities* – what are the requirements for cooling of the facilities and equipment, are there facilities meeting these requirements

6) *Fire Protection* – what alarms, detectors, suppression systems, etc need to be in place to protect this equipment

7) *Data Replication* – what is the desired method for data replication (Oracle replication, EMC SRDF, SQL Log shipping, etc), real time data replication vs static daily update and their respective cost implications, what other intervals of updates will be needed

8) *Site Plan* – what possible locations meet the requirements, obtain site plan for the most viable location including entry points for power, telephone, etc

Technology Considerations

There are several technical considerations which must be taken into account for each location. These requirements involve the use of load balancing vs. failover vs. backup.

- *Load Balancing* -- If load balancing is required what algorithm will be used (round robin, least connections, predictive, etc)?

- *Failover* -- If failover, is it manual or automatic, if automatic what mechanism: 3DNS in front of the Web servers to change the IP address automatically based on site availability or failover logic built into the applications?

- *Front End Vs. Backend* -- Is it required from the front end or backend? If data isn't changing too much, front end load balancing or failover is recommended. But if backend implementation is

NSE Disaster Recovery and Plan and Systems Back-Up

required, the data replication questions have to be answered.

- *Backup* -- If backup, what is the desired interval and data size, what is the method and what software and hardware to use, which offsite facility will store the data, how long will the backups be retained, how is sensitive data protected during storage, who has access to backups, what happens to backups when they are no longer needed, are mirrored drives used on the current hardware

Another aspect of any solution is including a Monitor device which will be the actual mechanism to failover from the primary to the secondary site in case of a disaster. Its purpose is to check if the primary site is up, if the database is up, and if the applications are running. If anything is detected as malfunctioning, it will failover to the backup site immediately. A popular solution in the United States is 3DNS software provided by *F5*.

Operations and IT Findings at NSE, CSCS and SEC

The DM research team found the following operations and IT findings in the NSE, CSCS and SEC.

Market Participants and Interactions

- 276 Listing/issuing companies interact with NSE and SEC to satisfy regulations for listing on the exchange.
- 39 Issuing houses act as investment managers in the market place. Some stockbroker firms are also issuing houses.
- Investors interact with stockbrokers who have to be affiliated with a licensed stockbroker firm. Investors issue buy/sell orders to the brokers.
- Stockbroker firms interact with NSE/CSCS to conduct transactions, settlement, and exchange transaction trading information daily.
- 15 Settlement banks hold the stockbrokers checking and trading accounts. A Settlement bank can represent multiple brokers but brokers can only be represented by one settlement bank.
- 37 Registrars setup as agents of Listing companies, issue instruments and verify certificates. They interact with CSCS and stockbrokers weekly for their exchange transaction information.
- Listing/issuing companies interact with Registrars for certificate verification.
- CSCS interacts daily with Settlement banks for zero-ing out the $ transactions.
- Settlement banks interact daily with Central Bank of Nigeria's banking clearing systems NIPSS and RTGS to clear checks and transactions.
- CSCS interacts daily with stockbroker firms for shares transactions and obliga-

NSE Disaster Recovery and Plan and Systems Back-Up

tion between the firms, changes to stockbroker clients, etc.

Trading Operations

Trading hours are from 10am to 12 noon daily. The hours can be extended based on circumstances. Start and end times are triggered manually. In 1999, transaction volume was near 300 transactions per day which has now grown to over 5,000 per day. It is further expected to grow to 7,000 – 8,000 / day within one year.

The actual trading begins with the certificates of the securities to be traded on the floor of the Stock Exchange being lodged with the stockbrokers. The shareholder signs transfer form which is submitted along with the share certificate to the stockbroking firm. The stockbroking firm lodges the documents with Registrars for signature verification/authentication and thereafter the Registrar submits verified certificate and the signed transfer form with two copies of certificate depository form to the depository of the CSCS within 24 hours, and also notifies the stockbroking firm of the lodgement. The shareholders can then sell all or part of their holdings through the stockbroking firm that processed the certificate lodgement with CSCS.

All trades are cleared by the netting process through the approved Settlement Banks whilst the dematerialized certificates are recycled to the Registrars within 48 hours. The CSCS sends information on trades to the respective Registrars to enable them to update their records with the new stock positions. The stockbroking firm informs the investor of the new stock position and settles the account with the investor. Refer to Annex I for summarized trading workflow.

To prevent erroneous trades or overtrading, a Trade Guarantee Fund has been setup to allow over trading to settle without cancellation of trades. This fund is a pool to which stockbroking firms contribute 100,000 nairas and the offending firm has to replenish the difference after its use. The Guarantee fund has been used only once since its setup.

IT Operations

NSE – Each trading floor of the NSE has a LAN. There is a WAN connecting five branches to the head office in Lagos via a combination of VSAT, Dial-up and the use of T1 lines. Over 70 stockbroking firms trade from their offices in Lagos. They are connected to the Lagos trading server via the T1 lines. All stockbrokers have to purchase their equipment and preloaded trading software from NSE.

NSE retains a technical staff of four full time technical employees to support the databases, the applications, apply updates and secure the backups for all of NSE. A consultant is also employed to maintain the network and provide tech support.

CSCS -- When shares are traded through CSCS, their physical certificates are automatically 'dematerialized' or cancelled thus creating e-certificates residing in the CSCS database. CSCS technical staff provides coverage for the IT systems 24x6x356 with

NSE Disaster Recovery and Plan and Systems Back-Up

Sunday being the day for maintenance windows or shutdowns.

SEC -- In 1999, the Management noted that the Commission was lagging behind the capital market and was not being driven by technology. IT consultants Deloitte & Touche were engaged to review and assess the existing IT situation and generate a strategy that will take the Commission to the level of being technology driven. Since then, a new Management team has been put in place and some of the IT initiatives were slowed down. In 2005, 5 of 19 planned IT tasks have been completed. The remainder tasks are in various stages of completion. The main hurdles appear to be funding as well as a new focus by Management.

Automated Trading and Depository Systems

Computershare Software Services Ltd has two key software products, Horizon and Equator (Stock Exchange management System SEMS). The Automated Trading System (ATS) of the NSE runs on the Horizon and CSCS on Equator. NSE Horizon and CSCS Equator are fully integrated towards Straight-Through Processing (STP) model. The STP model offers the end-to-end automation for the trading process within and between buy and sell supporting institutions, from the first placement of an order through final settlement.

Central Securities Clearing System

The Equator software on which the CSCS runs is a depository solution that is currently deployed in 33 exchanges including Poland, Egypt, Iran, Brazil, Romania, Japan, Canada and Cote d'Ivoire. The Equator has six integrated modules which support a wide variety of securities instruments in different markets. The modules are:

- Depository/Registry with corporate actions support
- Clearance and Settlement
- Administration and Billing
- Pledge Management (Collateral management)
- Borrowing/Lending
- Risk Management /Withdrawals

Equator supports multiple markets with different rule-sets, price discovery mechanisms, listing requirements, transaction types, settlement terms and policies. It supports a large list of security instruments including Equities, Rights/Warrants, Fixed Income, Commodities, Derivatives, Money Market instruments (T-bills, etc), Electronic IPOs (eIPO). It supports International Standards, Listed and unlisted markets, 9.9 billion Accounts currently, about 6 billion National Identification Numbers (NIN), Regional/Across the Border Identification Numbers, Delivery vs. Payment, Real Time Gross Settlement, Multilateral Netting (Cash), Trade for Trade (Securities). It supports multiple languages including English, French, Arabic, Japanese as well as multiple currencies.

Technical Details of CSCS systems include a Live System Server AS/400 9406 Model 820 with 200GB Disk space and 2GB RAM currently utilized at 20% capacity. Their Online Backup Server consists of the same

NSE Disaster Recovery and Plan and Systems Back-Up

hardware with an 8 disk storage array. Their off-site Backup Server is AS/400 9406 Model 50s with 175GB Disk space and 1 GB RAM. A redundant System Backup Server is the same hardware as the off-site server. Additionally, there are 25 workstations accessing the Live system server supported via Ethernet Network with TCP/IP.

For hardware, Symmetric Multiprocessor machines (SMP) are used with a redundant array of disks guaranteeing fault tolerance on the systems. The servers have integrated operating security management features which protect the confidentiality of the information content. The CSCS servers conform to the US Government C2 rating thus providing Trusted Computing Base (TCB) that implements extensive security provisions certified by the U.S Department of Defense. The systems are E-Servers internet enabled with Open Architecture. Full system auditing is done for historical reference on any transaction listing the date, time, source and user who affected it.

NSE Automated Trading System and Setup

Computershare Horizon is the Automated Trading System solution for NSE. The trading software was developed by Australian based Computershare Software Services, formally known as EFA Software Services Ltd of Canada. The software is client server, with one server license and unlimited broker client software installs, with client machines with TCPIP access. Maintenance is paid separately annually. The system cost about $600,000 to implement and surprisingly only took one month to rollout. The same system has been under rollout at an Egyptian exchange for 2 years now and is still not fully completed. The $600,000 price tag was funded by a grant from UNDP, United Nations Development Program.

The Automated Trading Solution Components include:

- One IBM desktop workstation with Windows XP per stockbroking firm
- Two servers RS6000 – one real time Production and one Backup server. Both are running on Oracle v 8.1.7 and AIX operating system
- Real time replication of the database is done via Sybase replication. The database servers act as Application, Middle tier/Components and Database device, housing all components
- Between the real time and the shadow box, there is a storage device in between with capacity of roughly 100GB that stores the actual data so neither server is the data bottleneck in case of failure.
- Failover is manual, someone has to press the button to fail over from the real database to the shadow database

As a middle ware residing on the DB server, there is a messaging system known as MHS, message handling system. It communicates with the workstations and the engine.

Three types of databases exist at NSE:

1) Trading databases described comprised of broker, listed companies,

NSE Disaster Recovery and Plan and Systems Back-Up

prices and price changes type of data residing on two RS6000 servers.

2) Independent separated local server which is updated manually at the end of each day with records of everything from the trading floor and keeps all the transaction history since 1996. It produces daily reports of the NSE activities. This server has compliance implications and as such should be included in any DR solutions.

3) The NSE RS6000 server is tightly coupled real time with the CSCS server for smooth trading. The trading database is synchronized with the CSCS database real time hence they back each other up. The trading database doesn't provide Names or NINs as the CSCS database but has all other data points.

SEC Connectivity and Setup

In 2005, the SEC implemented interconnectivity with the NSE and SEC remote branches. This enables SEC to carry out their surveillance role. Fiber optic line between NSE Lagos and SEC-Lagos Zonal Office (SEC LZO) was completed and VSAT connectivity was established between SEC LZO and SEC Head office in Abuja. In addition to monitoring from the HO in Abuja, SEC also has a workstation on the NSE trading floor in Lagos.

The surveillance module of the trading solution is utilized to catch large transactions or illegal sell/buy of shares. It is only available for access to one person (per entitlements) on the trading floor who manually monitors the transactions by viewing the screen and attempts to catch abnormalities for corrections. The tech admin at NSE also has access to the module for support purposes. SEC in Abuja is also performing the same monitoring through the VSAT link.

Trading Floors Network Connectivity and Setup

The trading floor in Lagos consists of about 140 desks on the floor equipped with IBM Windows 2000 PCs. Additional 20 stations are outside of the floor but still in the building accommodating stock broker firms located in the same building who are linked to the local LAN, and 90 stations are off site for brokers connecting via dial up, T1, PTO, VSAT, etc. Regardless of access, once connected, all brokers are trading real time. Downtime on the PTOs (Private Telephone Operators) channel is high as it is affected easily by weather conditions, and therefore should be looked at being replaced.

Three T1 leased lines support the remote traffic with about 30 concurrent connections per line. Multiplex equipment supports the 90 remote users by distributing the load over the three T1 lines. Duplicate network equipment has to be considered in DR solution

WAN network is established with LAN in Lagos and connectivity from the other branches to a RAS server residing on the Lagos LAN. The hardware is Cisco equipment, Cisco firewall, some Siemens hard-

NSE Disaster Recovery and Plan and Systems Back-Up

ware as well. Duplicate network equipment has to be considered in DR solution

The trading data center also consists of power generators to support trading hours between 10am and 12 noon each day.

Uninterruptible Power Supply UPS electricity large scale stabilizer is in the data center. Separate small stabilizers are installed per trading workstation so they can be isolated and treated.

Cooling systems keep the temperatures in the data center around 20 C.

NSE Online Trading Platform

The NSE Online Trading platform runs on Sybase Financial Fusion Server. The web based application and web servers are used by investors and stockbrokers to access real time market data as well as access their portfolios, client data and transactions. Also has ability for brokers to execute trades online however that module has not been turned on due to licensing negotiations still going on. The service is subscription based and when the user logs on, he is immediately authenticated and fixed messages are exchanged with the CSCS depository. This platform is independent of the NSE Computershare Trading System. The solution, including VSAT implementation, cost less then $300,000 and the cost was borne by Sybase with the agreement that Sybase will be paid overtime by subscription fees collected by the NSE. However, since 2003 implementation, Sybase has not received any payments and is unhappy with the NSE. Competing with Sybase on this project was a UK based company which was going to provide the solution 'for free'.

The hardware consists of one HP/Compaq web server and one Sybase adaptive server housing the application server and the database which is replicated real time data from the production database using Sybase replication. Backup has been implemented. URL is www.nigerianstockexchange.com.

Existing Backup and Recovery Strategies

The CSCS Backup strategy is conceived at an enterprise level for Consistency, Reliability, Extensiveness and Usability (7 years of CSCS operations with no down time). CSCS has full audit controls and disaster recovery of the databases. All database entries such as investor data, stockbroker transactions and settlement are journalled so that there is full commit and rollback. The current DR plan covers:

- Physical site (building and power)
- Daily Operations
- Physical equipment hardware
- Systems and systems software
- Communications

A Media Backup (Tape) of the databases containing all of the investor and transaction data at CSCS is done for Daily, Weekly and Monthly circles. All tape media are stored in fire proof cabinets on-site and a copy is stored off-site in Ikoyi.

Machine Backup at CSCS includes provisions for the following hardware Server backups:

NSE Disaster Recovery and Plan and Systems Back-Up

- Live System – runs nonstop 24 hours a day providing all required responses to transaction processing and inquiries. This allows for all trading activities and settlements to take place.

- On-Line Backup Server – is a replicate of the live system. It is meant to take over immediately if the live system fails. It requires minimal time to switch over (via manual failover mechanism). The backup is online and real time.

- Off-Line Backup Server – is a standby machine with the capability to replace any of the live or online backup servers.

- Redundant Backup Server – in the event of failure of any of the above servers, this system is to provide an immediate temporary solution without causing a complete and total breakdown.

- NSE Trading Server/NSE Trading Statements - is the source of the transactions to the CSCS at the trading floor of NSE, there is adequate backup of all transactions that can be reproduced into the Depository system so they serve as backup to each other.

Security provisions at CSCS include:

- Physical – the environment is fortified with steel braces well embedded for the protection of the vaults as defined by the external depository standards provided by IFC, Citibank New York. In addition there are special security service personnel attached to the office to prevent illegal and unauthorized access.

- System – the hardware systems are C2 compliant, definition by the DoD of USA.

Backup procedures in place at present at NSE include:

- Shadow box which provides on site backup of the server real time. This allows all stockbrokers on the Exchange floor to trade and log transactions.

- Synchronization with the CSCS database server so CSCS serves as a backup for NSE trading database.

- Daily backup of the database which stores all trading activities and transactions for the day is done on tapes which are kept in fire proof cabinet in the same building. The incremental daily backups start at 2pm and take about 1 hour.

- Weekly system backup on tape consisting of all application, data and OS components. This full backup begins at 2pm and can take up to 3-4 hours to complete.

Gaps in Existing Backup and Recovery Strategies

There are no major gaps in the backup and recovery facilities for the Central Securities Clearing System (CSCS). The facility in Ikoyi is brand new with state of the art equipment and facilities. It is housing a large number of the backup and recovery operations for CSCS and appears to properly adhere to Disaster Recovery standards and se-

NSE Disaster Recovery and Plan and Systems Back-Up

curity guidelines. The only operation not covered by the current strategy is the Business Continuity Planning. This means that in a scenario where the main CSCS office in Lagos has to shut down, the Ikoyi facility will recover and operate all databases and technology equipment but there are no provisions to accommodate staff and their daily operations for any period of time.

In comparison, the Nigerian Stock Exchange is missing any DR facility for its databases and equipment and also does not have a recovery preparedness and Business Continuity Plan (BCP).

The DM team is recommending for a knowledgeable team to put together the specifications for such a DR facility for NSE to include equipment and database recovery as well as business continuity plan of operations. Alternatively, the team should look at the feasibility and opportunity to partner up with CSCS to utilize or expand its Ikoyi facility to include DR procedures and operations for NSE.

Operating Environment at NSE and CSCS

NSE and CSCS are both situated in the same 24 story building in the middle of the congested financial center in Lagos. NSE and CSCS currently occupy floors 2, 3, 8 and 23. NSE is considering acquiring the full building. Sale of property and transfer rights in Nigeria may take up to 10 years to transfer officially due to governmental inability to handle such transactions given the current property rights and registrations in the country.

Building conditions are not favorable. There is no running water in the building as is the case for a good number of buildings in Lagos. The building has one fairly narrow staircase where just about two people can fit on a stair. It is an old building with weak air conditioning and overcrowded environment. Some NSE 8x 8 offices were occupied by 6 people. Significant risk exists for all people working in the building in case of fire.

Sufficient power is provided through four power sources:

1) Government NEPA is the main source of power for the building;

2) Generators run by consultants provide full backup for the building;

3) NSE owned generator provides full building support; and

4) CSCS owned two smaller generators provide support for CSCS only. Separate wiring and control switching already provided for alternative power. Uninterrupted power supply when there is power cut. A power engineering consultant is on retainer-ship to ensure clean, steady and stable power supply.

UPS and Stabilizers are sufficient. One main UPS services all servers and 60 workstations at CSCS and another UPS is at NSE. Two standby UPS can be manually triggered to take over.

The air conditioning seems inefficient in the building. However, the server rooms at CSCS and NSE are properly air conditioned

NSE Disaster Recovery and Plan and Systems Back-Up

and protected against dust. Cooling is set between 16C and 20C in the server rooms.

Smoke detectors and fire alarms are installed to alert of impending danger in the event of fire. Fire Extinguishers are available in the building and the members of staff have been trained to operate them.

C. Developmental Impact

Nigeria has an exciting and growing capital market and expectations about the NSE growth and transactions are in the double digits in the next two to three years. The DR project will provide a valuable alternative to the existing Exchange infrastructure in case of fire and also in case of any other type of emergency at the main trading floor location in Lagos.

By providing continuous service reliably, NSE will further enhance its image as one of the top exchanges in Africa and will encourage more investors to participate.

Development impacts include: increase in technology infrastructures, increase in utilization of higher end communication systems such as T1 lines instead of old fashioned VSAT or dial up and, increase in knowledge and experience with building the DR sites, further enhancing the technical knowledge base of the staff as well as helping the organizations develop best practices and procedures followed by much more developed exchanges in the world.

A few jobs will also be created for maintenance and updates of the DR site or a local contractor may be retained to provide the maintenance thus also expanding the activity in the local economy all leading to better profitability of the local companies and organizations.

D. Implementation Financing

To date NSE has financed its IT capital expenditures through UNDP grants, arrangements with vendors for future payments as well as internally generated funds. NSE operates at a surplus and is capable of funding at least part of the DR. It is also likely to seek donor and Central Government grants to meet its capital expenditures.

H. Evaluation Factors

E. U.S. Export Potential

Between NSE, SEC and CSCS, a lot of US technology is already utilized. Most of the server equipment is HP and IBM, desktop computers are Dell and HP, databases are Oracle, Sybase, and SQL, network and security equipment is Cisco, storage devices, operating systems ranging from Unix, Linux to Microsoft Server, 2000, and XP. Local companies provide the procurement and some non USA desktop boxes are in operation as well.

The expense for the physical DR logistics of building, power, generators, UPS, cooling, security guard services and other building utilities are all expected to be sourced through local firms able to provide all logistics and IT services

NSE Disaster Recovery and Plan and Systems Back-Up

Typical DR facility calls for duplicating the existing infrastructures and hardware already in place as it needs to ensure equal performance to the current production environments. To that end, a build out of a DR facility for NSE and CSCS will allow US based companies to provide hardware, software and even some services during the implementation stages. We estimate the total project would cost about US$2 million, of which about US$0.8 million worth of equipment, software and service potential for US suppliers.

A possible sub-project that we have identified during our visit is a certification of the NSE/CSCS IT infrastructure, security and data integrity. Expanding on the DR specifications and audit for build out of a complete environment, there is an opportunity for a large US consulting house to do a security audit of the exchange and its depository. Such audit and certification would include auditing the prevention, authentication, penetration, entitlements, database structures and break in responses as well as expose any data security and integrity issues. Correction of uncovered problems, expanding the security equipment in terms of hardware and software as well as testing and training of the staff can also be an integral part of the audit and certification. There is also a developmental impact in that the final audit certification would solidify the image of the exchange as secure and ready to support larger capital market activity with integrity, reliability and availability. We estimate this sub project to engage a couple of consultants for one month as well as result in additional security hardware and software purchases from US suppliers. The estimated total US export opportunity is upwards of US$0.5 mil based on how much security equipment, software, licences and certificates have to be procured to certify the exchange.

The following companies would benefit from this business:

Networking routers, peripherals, and associated technologies
CISCO, EMC, F5, BigIP, Motorola, IBM, APC

Software Companies
Oracle, Microsoft, Sybase, VeriSign

Consulting companies
DPMS, NCR, Accenture, Deloitte & Touche USA LLP subsidiaries

Data storage manufacturers
HP, EMC

F. Foreign Competition

U.S. telcommunications and networking companies will face competition from European conglomerates such as Siemens, Erikson, and Alcatel who are well established in the Africa region. On the software front Computershare Software Services from Canada, MIT from Sri Lanka, SAP from Germany and Tata Consultancy Ltd India based, all companies capable of competing as application and equipment providers. On the consulting front competition includes Nigerian based AWD&T as well as Progenics Corp which has provided NSE with IT consulting services in 2003 and is currently servicing a few IT infrastructure projects at SEC.

NSE Disaster Recovery and Plan and Systems Back-Up

The future sponsors of the DR project are likely to undertake the entire procurement process through open competition, where U.S. companies will be eligible to apply. If U.S. consultants develop the specifications and rollout plan, it is likely that the U.S. companies would be better placed to win the resulting contracts.

G. Impact on the Environment

The project would not have any adverse impact on the environment. But we would like to note the potential for construction work which may take place for alterations to an existing building or construction of a new facility. Certainly any future research and studies should address potential environmental impact factors if such are uncovered during the study.

H. Impact on U.S. Labor

The project would not reduce the number of employees of any U.S. company and will not displace any U.S. company outside of the United States.

The project is particularly beneficial for U.S. exports, as all ICT equipment and software are likely to be made by U.S. manufacturers and wholly produced in the United States with U.S. labor.

I. [illegible]

There are a number of firms capable of performing this study. The successful firm should commit individual team members who can work with Construction Engineers and Architects and possess a combination of the following qualifications (total points to be allocated 100):

Technical Qualifications

- Demonstrated capability of developing medium to large server computer network architectures (15%).
- Demonstrated experience in understanding and designing disaster recovery, identifying equipment, design of procedures and rollout plans, best practices in design considerations, general facility design (MDF, IDFs) preferably in developing countries (30% percent).
- Experience in the security, database structures, circuits, network connectivity and project management including experience in developing countries (30% percent).

Regional Qualifications

- Experience conducting corporate or national level IT assessments, preferably in the Africa region (15%).

Project Management Qualifications

- Proven project management experience interacting with senior level government officials and with handling difficult political situations (10%).

The following positions should be presented for this assignment. The bidder may provide other qualified individuals as they see appropriate:

NSE Disaster Recovery and Plan and Systems Back-Up

DR Technical Architect

- Single point responsibility for overall coordination and quality of the Feasibility Study.
- The DR Technical Architect must have a strong technical and mechanical engineering background and skills with an in depth understanding of the technical, business and construction issues involved in Disaster Recovery facility building.
- The candidate must possess a strong background in business continuity management and disaster recovery assessment and planning. Demonstrated experience with risk evaluation and control, business impact analysis, business continuity strategy and development, emergency response and operations, developing and implementing business continuity plans, developing Technology and Business process recovery strategies and crisis communication planning a required.
- Required skills in development of detailed plans and specifications for DR facilities, equipment and procedures as well as creating project schedules and leading teams.
- General understanding of security and systems change control concepts and understanding of building layouts are also preferred.
- Ideally the candidate should have a Mechanical Engineering degree and minimum of 7 years of consulting or operating expertise in disaster recovery or data center facility building, experience dealing with Building Architects and construction plans and proven ability to manage consulting assignments of this nature.
- CBCP or MBCP certification preferred. Equivalent experience as 9/11 disaster recovery is preferred as well as recent experience in West Africa (last 7 years) should be presented.

Network/Security/Database Engineer

- Multifaceted experience working in networking, security, applications and system design, and equipment management.
- The individual should have experience running and supporting data center operations with database storage devices as well as experience with IT infrastructure planning, implementation, systems management and support.
- Areas of expertise should be with IP networking, telecommunications, LAN/WAN implementation (VPNs, TCP/IP, DSL, VLAN, etc.), routers and current Microsoft Operating Systems and Back Office Platforms. Also valuable are experience with corporate virus protection products, business class Backup Systems, firewalls, VPN client and tunnel technologies, circuits, routing protocols and related technologies including BGP4, OSPF; DNS and load balancing technologies (SSL, Cookies), experience with Cisco-based design and configuration, experience with using data analyzers (both IP and serial).
- Requires at least a Bachelors degree in Computer Science or Electrical Engineering, as well as five to ten years industry experience in a Network Operations Management or Network Engineering role, or equivalent combination of education and experience.
- Certifications such as MCP with MCSE equivalent competencies or current MCSE is ideal. MCSE with additional complimentary Microsoft certifications such as MCDBA, or some Oracle and Cisco certifications are highly desirable.

NSE Disaster Recovery and Plan and Systems Back-Up

Telecom Engineer

- A minimum of 5 years of experience working on connectivity projects. The individual should have worked with various telco networks, routers and equipment and be familiar with telecom corporate best practices and backup strategies.
- The individual should have been instrumental in planning the telecommunication infrastructure of a new facility as well as overseen or at least participated in the implementation of the selected vendor networks and systems.
- Extensive knowledge of data, broadband, radio or satelite communication concepts and technologies is required. AT&T and Cisco knowledge is required. Background in communications and signal processing is needed.
- Requires at least a Bachelors degree in Computer Science or Electrical Engineering, as well as five to ten years industry experience in a telecommunications and infrastructure corporate operations
- Telecom Engineer with knowledge and experience in developing countries and Sub Sahara region while not a specific requirement would be a plus

Grantee's Request

The NSE has requested that USTDA help it design and implement a Disaster Recovery Plan and Emergency Backup for the Stock Exchange.

J. Justification

USTDA involvement is justified on the basis of the export potential.

In addition to providing valuable technical service and solutions to NSE to facilitate its reliability, availability and future growth, we believe that USTDA's support would open opportunities for U.S. companies for about *US$800,000* and would help displace competition from South African and European companies.

If U.S. consultants develop the rollout plan then it is highly likely that the current use of U.S. technology (Oracle, IBM, HP, etc.,) would continue and would expand. On the other hand, if the NSE decides to hire European or other consultants to develop this plan, there is a risk that the technology would be favored to suppliers from Europe or other countries, including South Africa.

If USTDA finances the feasibility study for the DR project, USTDA has a ground floor opportunity to be the first technology advisor to NSE for such a project. There has been no research, scoping or planning done to date for such a project and NSE has made no commitment to any companies that they would be hired or be involved. If the rollout plan is designed by U.S. consultants (funded by USTDA), the current use of U.S. technology (Oracle, IBM, HP, etc.,) would continue and would expand and as well as the involvement of U.S companies. If USTDA does not finance this rollout plan, NSE is likely to use existing suppliers and local advisors for help in developing the rollout plan, and the resulting procurement could be geared toward non-U.S. suppliers.

NSE Disaster Recovery and Plan and Systems Back-Up

K. Terms of Reference and Budget

Aim of Terms of Reference

This Disaster Recovery (DR) Technical Assistance (TA) will address the technical and business requirements for a DR facility for the Nigerian Stock Exchange (NSE). It shall review existing studies, the manual and automated backup systems in place, and existing hardware and communications infrastructure at the NSE and the Central Securities Clearing System (CSCS). The TA will develop a strategic plan, specifications, and an implementation plan for a Disaster Recovery facility. The Contractor will ensure that any recommended procurements can be integrated with existing hardware, communications infrastructure, applications and databases.

The DR Technical Architect and the Network/Security/Data Engineer's analysis will be used when the building architect and his firm commence building construction, building modification or the lease of an appropriate facility, in order to bring it up to DR plan site specifications.

Tasks and Scope of Work

Task 1: Review Existing IT Systems and Plans

The Contractor shall further research and validate the technical findings and recommendations in the Definitional Mission report provided as Annex II in the Request for Proposals. The Contractor shall identify mission-critical IT systems, applications and hardware at the Lagos headquarters of the NSE and CSCS. The Contractor shall review the following areas to gain a thorough understanding of the existing technologies and infrastructure and how information technology is used by the NSE and CSCS:

- Application /Systems Design
- Development
- End-to-End Authentication
- Database Authentication
- End-to-End Authorization
- Operating Environment
- Support
- Networking
- Firewalls
- Monitoring/Logging

Task 2: Review Backup, Recovery and Security Related Operations and Business Procedures

The Contractor shall carefully review and assess capabilities of existing backup facilities, systems, hardware, applications, network procedures and communications infrastructure to assess the disaster recovery needs and gaps in existing backup and recovery procedures. The Contractor shall also review present backup and recovery operations and business procedures related to the trading operations and IT infrastructure at Lagos NSE/CSCS Headquarters. The team shall gain a thorough understanding of all relevant aspects of:

- Business Continuity
- Backups
- Appliance and IT Security
- Physical Security

NSE Disaster Recovery and Plan and Systems Back-Up

This analysis shall identify key operations, security gaps and/or business areas that are not properly planned in terms of recovery of operations, backup and security.

Task 3: Current State Assessment Document and Presentation

The Contractor shall conduct a working group meeting with the NSE and CSCS IT/MIS personnel in order to review the findings from Tasks 1 and 2, and gather feedback to be used in the development of the DR Strategic Plan.

Deliverable: The Contractor shall prepare a Current State Assessment Document and Presentation based on the analysis from Tasks 1 and 2. The Document and Presentation shall provide a current state analysis of NSE current backup and recovery initiatives, CSCS current backup and recovery initiatives, mission-critical trading operations, and business processes under evaluation at the NSE for business continuity and disaster recovery. The Contractor shall also detail the findings of the existing infrastructure review. This assessment shall help determine key business and operational areas and/or functions targeted for disaster recovery. The assessment shall assist in articulating the overall DR Strategy and Implementation Plan.

Task 4: DR Strategic Plan and System Requirements

Deliverable: The Contractor shall prepare a DR Strategic Plan for the NSE to support its trading operations and disaster recovery goals. The DR Strategic Plan shall outline the needs, goals, security, and performance objectives for the future disaster recovery site as agreed by the Grantee. It shall contain the detailed technical requirements, business and operational requirements, and any dependencies and assumptions. All network, communication, building construction, hardware, and application requirements shall be included in the Strategic Plan. The Strategic Plan shall also include the following:

A. Redundancy Purpose. The Contractor shall evaluate the technical, business, and logistics information for preparedness in case of fire. The Contractor shall draft disaster and contingency plans allowing for system redundancy and backup in the event of a building fire. The Contractor shall clearly define the technical decisions related to Load Balancing vs. Failover vs. Backup and the systems which will be affected by each chosen method.

The Contractor shall validate that the main threat to the operations of the Nigerian capital market at this time is the threat of fire, electrical or accidentally started. The office spaces are overcrowded and outside help cannot be relied upon due to the location of the building, the height of the building and the gridlock traffic pattern in the district making it hard to access. Other factors weighing negatively are the exit unfriendly building design, the lack of running water in the building or the vicinity thereof, as well as the lack of experience in extinguishing high rise building fires by the Lagos Fire Department.

NSE Disaster Recovery and Plan and Systems Back-Up

The secondary objective of the redundancy is to provide a mechanism for continuous trading and support of the exchange in case of failure of the main building or main equipment. Business continuation of processes and services is critical for an expanding exchange where volume transactions are doubling each year, capitalization is growing at 30% annually, and the expected new listings and new money coming to the capital market place is expected to double in the next three years.

B. Service Level Agreement SLA Expectations. The Contractor shall research, evaluate, and make recommendations on the following SLA expectations in order for the operations and data to be fully recovered in real-time status:

1. Real-time replication of both independent production and DR data centers. The recommended option shall include two physical data centers, each running independently with only Network failover. When data is sent, it shall be sent to both centers at the same time, independently. The only common element shall be the connectivity to the corporate backbone network

2. Automatic failover of all systems to the DR facility.

3. Automatic failover for all NSE databases and servers.

4. Automatic failover to CSCS off-site backup server and depository.

5. Full availability of databases so that all data and history is available.

6. The percentage of NSE operations that need to continue in case of disaster is 30%.

7. The Performance of the DR facility and equipment in relation to the performance of the Production environment must match 100%.

8. Uptime of 99% and availability of the DR facility in case of failover and establishment of maintenance windows for emergency support.

9. A Support team of technicians in order to provide tech support and guidance with the applications and servers in the DR facility. The team shall define the composition of the team and their qualifications.

10. Business applications such as Computershare Horizon and Equator applications for trading, settlement and surveillance and the need for uninterrupted service

11. Other applications and the target needs for service and update such as the Sybase Fusion server for online trading and account management and investor information. The Contractor shall define the specific needs.

12. Twenty workstations preloaded with trading software that need to be located in the new DR facility so trading in Lagos can continue.

NSE Disaster Recovery and Plan and Systems Back-Up

13. Operational NSE and CSCS applications. The Contractor shall define all of the necessary operational applications.

C. Networking, Connectivity and Circuits. The Contractor shall:

1. Define the network, network connectivity and the proper security equipment necessary after a DR failover. It will allow the market operators such as investors, brokers, settlement banks, SEC and remote branches and trading floors to connect to the NSE's DR facility. The network connectivity target is 100%. The LAN or WAN must be capable of supporting the transaction volumes generated by the application software based on the trading and settlement volumes of the Exchange.

   The network shall conform to international standards. It shall be capable of expanding to accommodate future growth of participants and transaction volume. It shall enable the addition of extra communication links, the addition of extra processing power for network nodes, and the addition of new network notes and the relocation or expansion of existing nodes.

2. Define the network design that will allow it to operate even if communications links become unavailable.

3. Define the remote access abilities requirements that will allow trading from the other regional branches and trading floors to continue. Remote Access Server RAS is certainly one option. Alternatively, the network proposed should permit any end user in any office to access the trading and settlement systems as well as permit the transmission of electronic mail to any registered user on the network.

4. Define the data protocols and data transfers over the network and the internet.

5. Define the circuits that should be installed in order to handle the data replication traffic as well as 50% of the current production load and throughput.

6. Define the types of communication and telecommunication connectivity required to support the connectivity to the facility. Define all the equipment including routers and multiplex equipment that will be needed for navigating the network traffic. Some communication options in Nigeria include T1 leased lines, VSAT or Fiber optics.

7. Define equipment capable of being switched over to a backup data communication link using high speed (i.e 56Kbps minimum) dial-up lines. Define maximum data throughput between all major sub systems and components. Define both LAN and WAN throughput.

NSE Disaster Recovery and Plan and Systems Back-Up

8. Provide a Network Management System if network load and performance are of importance to Grantee. This shall cover the entire network and provide line loading, performance, and error and throughput measurement with continuous aggregate figures on data throughput between all nodes so that potential difficulties can be predicted and preventive maintenance performed.

9. Define the data transmission on the internal and external networks in order to support authentication of network terminals and workstations and prevent unauthorized monitoring of network transactions. This shall also support encryption / decryption techniques. Define a file transfer system that can provide error free transfer between systems with logging of file transfer requests, actions and failures. Ensure international transfer protocols are utilized.

D. Power Consumption. The Contractor shall define the power equipment required for the DR facility considering the guidelines that all processors, disks and communications equipment require computer-grade Automatic Voltage Regulators providing 220 volt 50 Hertz power supply, Automatic shutdown circuits in case of unit failure, and a maximum of 1 nanosecond response time.

Power generators for the full facility as well as duplicate backup generators should be available for the building.

A main Uninterruptible Power Supply (UPS) shall support the data center and a duplicate UPS shall be provided for manual failover.

Stabilizers for the data centers and the workstations will be necessary.

Vendors must define the power requirements for all equipment to be supplied. This should include voltage and voltage tolerance requirements, total power consumption, electrical grounding requirements, conductor sizes, and any other special requirements. The Contractor shall determine the number of power outlets required at the central site and at participants' offices.

E. Cooling Capabilities. The Contractor shall define the temperature which should be maintained at the DR facility and the equipment that needs to be procured to allow for prolonged and strong air conditioning and ventilation in the building.

F. Fire Protection. The Contractor shall outline the conditions of the DR facility in terms of running water in the building as well as the neighboring area and buildings. The Contractor shall define the number fire extinguishers that should be put in place and their locations in the rooms and hallways of the building. The Contractor shall define the staff training necessary to educate and train the personnel in fire emergency procedures and handling of necessary fire extinguishers and other safety equipment.

G. Data Replication. The Contractor shall:

NSE Disaster Recovery and Plan and Systems Back-Up

1. Define the data replication for the facility. This shall involve synchronous ongoing real time data replication if the DR facility is within 20 cable miles of current NSE/CSCS location. Some methods to select from include Oracle replication, EMC SRDF, SQL Log shipping.
2. Define the type and media of the daily updates such as tapes, diskettes and via web.
3. Define the type and media of the weekly updates such as tapes, diskettes and via web.

H. Site Plan. The Contractor shall define the type of facility, construction details, location, as well as building logistics that align with DR facility requirements.

1. The Contractor shall determine the location of the secure facility which needs to be allocated. The facility should have its own generators, stabilizers, UPS, running water, guards and security-controlled building access. Alternatively, the Contractor shall define the additions or modifications necessary to an existing facility such as the CSCS DR facility in Ikoyi. If a new building is required, the building should be in mainland Lagos.

2. The Contractor shall define the general facility conditions and identify special needs such as steel reinforcement of the roof, etc.

3. The Contractor shall define the power and telephone lines requirements for the facility.

4. The Contractor shall define the emergency procedures and the training for the NSE and CSCS staff to react and operate in reduced capacity.

5. The Contractor shall define the functions of the technical staff and training required to operate the equipment and DR failover and provide emergency support

6. The Contractor shall develop the business continuity plan with effective contingency and business continuity strategy for mission-critical business operations and systems, including trading applications, trading processes, equipment and mission-critical staff.

7. The Contractor shall define the type of personnel and the necessary skills and qualifications required to complete the DR project.

8. The Contractor shall define a target schedule for practice of emergency procedures.

Task 5: DR System Specifications

The Contractor shall provide sufficient details of specifications of hardware, software, security equipment, network and communications infrastructure equipment, applications, and any other equipment that may be required to meet the Systems

NSE Disaster Recovery and Plan and Systems Back-Up

Requirements outlined in the DR Strategy Plan. These specifications will be used in the bidding/procurement process and shall therefore be as accurate as possible given the requirements, dependencies, and assumptions of the DR project. Overall recommendations for the construction of the DR facility or modification of an existing facility, integration with existing systems, the DR Plan, and system security will be in terms of key performance indicators and functional specifications based on the Contractor's knowledge of what is technically feasible. The Contractor shall be careful not to provide system specifications to a level of detail that is "vendor-specific". The proponents will have to prove that the components of their proposed system can meet these specifications.

Deliverable: The Contractor shall prepare and submit adequate documentation for the work performed during this task, including the general and technical DR specifications.

Task 6: Implementation Plan

Deliverable: Taking into account the DR Strategic Plan containing the System Requirements and the System Specifications document, the Contractor shall create a phased implementation plan for the Disaster Recovery Project that includes a procurement schedule for the planned implementation of all elements of the facility in Lagos. This implementation plan shall incorporate any assumptions about the schedule and dependencies impacting the schedule. The Plan shall list each of the main tasks, the scope of work of each with start and ending estimates, and the duration of each task.

Task 7: Supplier Identification

The Contractor shall identify potential suppliers of the computer software and hardware to include specifications, quantities, minimum performance characteristics (at a minimum two vendors each) and estimated costs from different procurement sources.

Deliverable: The Contractor shall obtain detailed information from a variety of vendors that identifies the product, specifications, merits, installation requirements, warrantees, and costs for each of the recommended items or services. This information shall be in sufficient technical detail that the Grantee can make informed, responsible decisions regarding product or service procurement. The Contractor shall identify potential sources of supply of the equipment, including U.S. sources of supply, in accordance with Clause I of Annex II of the Grant Agreement.

Task 8: Development Impact Analysis

The Contractor shall report on the potential development impacts for the project in the Host Country of Nigeria. While specific focus should be paid to the immediate impact of the DR Project, the Contractor will include, where appropriate, any additional developmental benefits of the Project, including spin-off and demonstration effects (such as 'Security, Reliability and Data Integrity Certification of the Exchange'). The Contractor's analysis of potential benefits shall be as concrete and detailed as possible. The development impact factors are intended to provide the Project's decision-makers and interested

parties with a broader view of the Project's potential effects on the Host Country. The Contractor shall provide estimates of the Project's potential benefits in the following areas:

a. Infrastructure / Industry. The Contractor shall provide a statement on the infrastructure impact giving a brief synopsis.

b. Market-Oriented Reforms. The Contractor shall provide a description of any regulations, laws, or institutional changes that are recommended and the effect they would have if implemented.

c. Human Capacity Building. The Contractor shall address the number and type of positions that would be needed to implement, manage, and operate the proposed Project as well as the number of people who will receive training and a brief description of the training program.

d. Technology Transfer and Productivity Enhancement. The Contractor shall provide a description of any advanced technologies that will be implemented as a result of the Project. The Contractor shall provide a quantitative description of any efficiency that will be gained.

e. Other. The Contractor shall identify any other developmental benefits of the Project, including any spin-off or demonstration effects.

Task 9: Environment Impact

The Contractor shall perform a preliminary review of the Project's environmental impact with reference to local requirements and those of financial investors. This review shall identify potential negative impacts, discuss the extent to which they can be mitigated, and develop plans for full environmental impact assessment if and when the Project moves forward to implementation stage.

Task 10: Working Group Meeting and Presentation

The Contractor shall prepare for and conduct a meeting to present, review and summarize the information developed in the foregoing Tasks. The Contractor shall present the Grantee with a draft report including all of the aforementioned deliverables and assist with details as may be required.

Task 11: Final Report

The Final Report shall be a substantive and comprehensive report of work performed to carry out all of the tasks set forth in the Terms of Reference and shall include, among other things, an Executive Summary and all deliverables. Each task of the Terms of Reference shall form a separate chapter of the Final Report.

The Final Report shall also include a comprehensive list of suppliers, including potential sources of U.S. equipment and services, relevant to the implementation of each component of the Project as outlined in the Study.

The Contractor shall submit the Final Report in English. The Contractor shall provide

NSE Disaster Recovery and Plan and Systems Back-Up

five (5) hard copies and one (1) electronic version of both the confidential and public versions of the *Final Report to the Grantee* and shall provide copies to USTDA.

Budget for Technical Assistance

The budget is included in Annex I. The budget is based on the TOR for the Contractor's portion of the work only.

The work will have to be performed on site in Nigeria as their specific requirements of NSE and CSCS existing and future DR infrastructures have to be detailed and planned for implementation. The team can only perform such research and documentation onsite. Only some PMO (Project Management Office) tasks as well as the Final report can be written in the USA.

M. Recommendation

USTDA involvement in this project is justified on the basis of the export potential and the opportunities for US consultants. The development impact includes readiness for Security, Reliability and Data integrity Certification of the Nigerian Stock Exchange.

It is Computer Frontiers' recommendation that USTDA fund some portion of this FS project as described in the Terms of Reference. Computer Frontiers' estimate (budget) for the cost to implement the Contractor's portion of this TOR is $236,410.

NSE Disaster Recovery and Plan and Systems Back-Up

Annex I: Budget for Nigeria Disaster Recovery Technical Assistance to NSE

	DR Technical Architect	Network/ Security/Data Engineer	Telecom Engineer	Sub Totals	
Daily Rate- US$	$1,200.00	$1,000.00	$900.00	Days	Cost US$
Task Description					
Task 1: Review Existing IT Systems and Plans	7	7		14	15,400
Task 2: Review Backup, Recovery, Security	4	4		8	8,800
Task 3: Current State Assessment	4	4		8	8,800
Task 4: DR Strategic Plan & System Requirements	10	10	10	30	31,000
Task 5: DR System Specifications	3	3	3	9	9,300
Task 6: Implementation Plan	2	2	2	6	6,200
Task 7: Supplier Identification	1	3	3	7	6,900
Task 8: Development Impact	2	1	1	4	4,300
Task 9: Environmental Impact	1	0	0	1	1,200
Task 10: Working Group Meeting	10	10	3	23	24,700
Task 11: Final Report	7	5	3	15	16,100
Total Days	51	49	25	125	
Total Days on Location	44	44	10	98	
Total Labor Cost					[illegible]
Other Direct Costs	Type	Days	No People	Unit Cost	Total
Airfare RT	Trip		3	2,500	7,500
Hotel	Day	98	3	220	64,680
Meals/Per Diem	Day	98	3	95	27,930
Ground Transportation / Car services	Vehicle	40		40	1,600
Internet access/Copies/phone/misc	Day	98		20	2,000
Total Direct Costs					[illegible]
Total Direct Cost for Technical Assistance					[illegible]

Computer Frontiers

12-15-09;10:22AM;GIT INC ;8139734370 # 35/ 35