PN-ACC-416

Business Continuity Plan - Final report on Stage One (Telecom)

Financial Institutions Reform and Expansion (FIRE) Project

February 1997

Financial Institutions Reform and Expansion (FIRE) Project
US Agency for International Development (USAID/India)
Contract #386-0531-C-00-5010-00
Project #386-0531-3-30069

Price Waterhouse LLP
1616 North Fort Myer Drive
Arlington, V A 22209
Tel. (703) 741-1000
Fax (703) 741-1616

Financial Institutions Reforms
and Expansion (FIRE) Project

128 T V Industrial Estate
Worli, Mumbai 400 025

Telephone 4946630, 4963599
Fax (91 22) 4963555

Price Waterhouse LLP

12 February, 1997

Dr R. H Patil
Managing Director
National Stock Exchange of India Limited
Mahindra Towers, "A" Wing, 1st Floor,
RBC, Worli,
Mumbai - 400 018

Subject : Report for Stage one of the Business Continuity Plan - Telecommunication Department

Dear Dr Patil,

As part of our contract with the US Agency for International Development, Contract #86-0531-C-00-5010-00, Project #86-0531-3-30069, we have developed with your staff the first two stages of the Business Continuity Plan (BCP). Stage 1, which is the Business Impact Analysis - with the exception of the section on telecommunications-was delivered to you on October 9, 1996

The section on Business Impact Analysis for Telecommunications is attached to this letter This report was done with the help of a telecom expert from Citibank

This section on Telecommunication includes

- Recovery time scale analysis for the functions of the Telecommunications department and identification of recovery resources for the critical functions
- Operational risk assessment for Telecommunications resources

We have validated this information with your staff in the Telecommunications department

We would like to bring to your notice that there are certain operational threats to Telecommunications equipment such as failure of satellite, failure of transponder, failure of antenna, the recovery from which may not be accomplished within the required time-frame for business recovery because of certain Government regulations

For further clarifications, please contact Mr Walter Pugh, Mr Bimal Bhavanani or me at telephone no 496-3599 or fax no 496-3555

Thank you

Sincerely yours,

W. DENNIS GRUBB
Principal Consultant Capital Markets

cc Mr. Ravi Narain
Deputy Managing Director
National Stock Exchange of India Limited
Mumbai

cc Mr Satish Naralkar
Vice President
National Stock Exchange of India Limited
Mumbai

cc Mr L K. Singhvi
Sr Executive Director
(FIRE Project Coordinator)
Securities and Exchange Board of India
Mumbai

C

TABLE II-A-1 - Functions and Recovery times

Functions and Recovery times

Details	One Hour	Same Day	Next Day	Seven Days	Thirty Days
Department : Telecom					
Business Related operations					
VSAT network	√				
X.25 switch network	√				
Help desks	√				
Dialup network			√		
Internet Web site			√		
Notes mail system				√	
BBS / RAS			√		
Corporate Network			√		
Infrastructure related operations at active site/s					
LAN maintenance	√				
EPAX/EPABX maintenance	√				
Telephone maintenance	√				
Liaisoning with external agencies					
Liaise with external agencies	√				
Commercial activities					
Commercial activities			√		

Recovery Times	Number of functions to be recovered
One hour	7
Same working day	Nil
Next working day	5
Seven days	1
Thirty days	Nil

TABLE II-A-3 - Critical Functions Matrices

Department : Telecom

Criticality Time period for suspension	Low	Medium	High	Very high
for an hour	Business related Operations • Notes Mail system Commercial Activities	Business related Operations • Internet web site • BBS / RAS	Business related Operations • Dialup network	Business related Operations • VSAT network • X 25 switch network • Help desk Infrastructure related Operations at Active site(s) • LAN Maintenance • EPAX & EPABX Maintenance • Telephone line Maintenance Liaise with External agencies

TABLE II-A-3 - Critical Functions Matrices

Department : Telecom

Criticality Time period for suspension	Low	Medium	High	Very high
for a day		Business related Operations • Notes Mail system	Business related Operations • BBS / RAS • Internet web site Commercial Activities	Business related Operations • VSAT network • X 25 switch network • Help desk • Dialup network Infrastructure related Operations at Active site(s) • LAN Maintenance • EPAX & EPABX Maintenance • Telephone line Maintenance Liaise with External agencies

TABLE II-A-3 - Critical Functions Matrices

Department : Telecom

Criticality Time period for suspension	Low	Medium	High	Very high
for a week		Business related Operations • Notes Mail system	Business related Operations • BBS / RAS • Internet web site	Business related Operations • VSAT network • X 25 switch network • Help desk • Dialup network Infrastructure related Operations at Active site(s) • LAN Maintenance • EPAX & EPABX Maintenance • Telephone line Maintenance Liaise with External agencies Commercial Activities

TABLE II-A-3 - Critical Functions Matrices

Department : Telecom

Criticality Time period for suspension	Low	Medium	High	Very high
for a month			Business related Operations • Notes Mail system • BBS / RAS • Internet web site	Business related Operations • VSAT network • X 25 switch network • Help desk • Dialup network Infrastructure related Operations at Active site(s) • LAN Maintenance • EPAX & EPABX Maintenance • Telephone line Maintenance Liaise with External agencies Commercial Activities

TABLE II- B-1 - Recovery Within an Hour

Department : Telecom

Number of Functions/ Activities : Seven

Function	Systems Resources	Telecom and Non system Resources
VSAT network	1 PCs 2 MS Office 3 Printers	1. Direct lines/ STD 2 Copiers 3 Fax machine 4 Hub Baseband equipment 5. Hub RF equipment 6. NMS equipment 7 Idacom Analyser 8 Spectrum Analyser 9 Test VSATs 10. Marconi Power meter 11 UPS 12 AC equipment 13. Dehydrator 14. Exhaust fan 15. Thermostat controller
X.25 switch network	1 PCs 2. MS Office 3. Printers	1. Direct lines/ STD 2 Copiers 3. X.25 equipment 4. NMS system 5. UPS 6. AC equipment
Help desks	1 PCs 2 Printers 3 MS Office 4 LAN connections	1 Direct lines/ STD 2 Copiers 3 Fax machine 4 EPABX system 5 AT&T IVR equipment 6 Control terminal

TABLE II- B-1 - Recovery Within an Hour (Continued)

Department : Telecom

Number of Functions/ Activities : Seven

Function	Systems Resources	Telecom and Non system Resources
LAN Maintenance	1 PCs 2 Printers 3. MS Office 4. Server equipment 5 LAN connection	1 LAN Manager 2 LAN/WAN Analyser 3 Ethernet Hub 4 Ethernet Switch 5 Ethernet Cables 6. Ethernet I/O outlets 7 Ethernet Patchcords 8 Ethernet Patch panels 9 Ethernet mounting cords 10 LAN handheld Microtester
EPAX/EPABX Maintenance	1. PCs 2 Printers 3 MS Office	1 Direct lines/ STD 2 Copiers 3. Fax machine 4 EPABX system 5. Modems 6. Maintenance s/w
Telephone line maintenance		1 Direct lines/ STD 2 Krone tool 3. Telephone test instrument
Liaise with external agencies		1 Direct lines/ STD

TABLE II- B-2- Recovery by the next Working Day

Department : Telecom

Number of Functions/ Activities : Three

Function	Systems Resources	Telecom and Non system Resources
Dialup Network	1 PCs 2 Printers 3 MS Office	1 Direct lines/ STD 2 Modems 3 NMS system
Commercial Activities	1. PCs 2 Printers 3 MS Office 4 LAN connection	1 Direct lines/ STD 2. Copiers 3 Fax machine

TABLE II- B-3- Recovery Within Seven Days

Department : Telecom

Number of Functions/ Activities : Two

Function	Systems Resources	Telecom and Non system Resources
Notes mail network	1 PCs 2 Printers 3 MS Office 4 Notes Server 5 LAN connection	1 Direct lines/ STD 2 Leased lines / DAMA VSATs 3 Modems
BBS / RAS	1 PCs 2 Printers 3 MS Office 4. BBS Server equipment 5. Eicon Server equipment 6 LAN connection	1 Direct lines/ STD 2 Modems

TABLE II- B-4- Recovery Within Thirty Days

Department : Telecom

Number of Functions/ Activities : One

Function	Systems Resources	Telecom and Non system Resources
Internet Web site	1 PCs 2. Printers 3 MS Office 4 Web Server 5 Firewall Server	1 Direct lines/ STD 2 Leased line 3 Modems

TECHNOLOGY BEHIND NSE

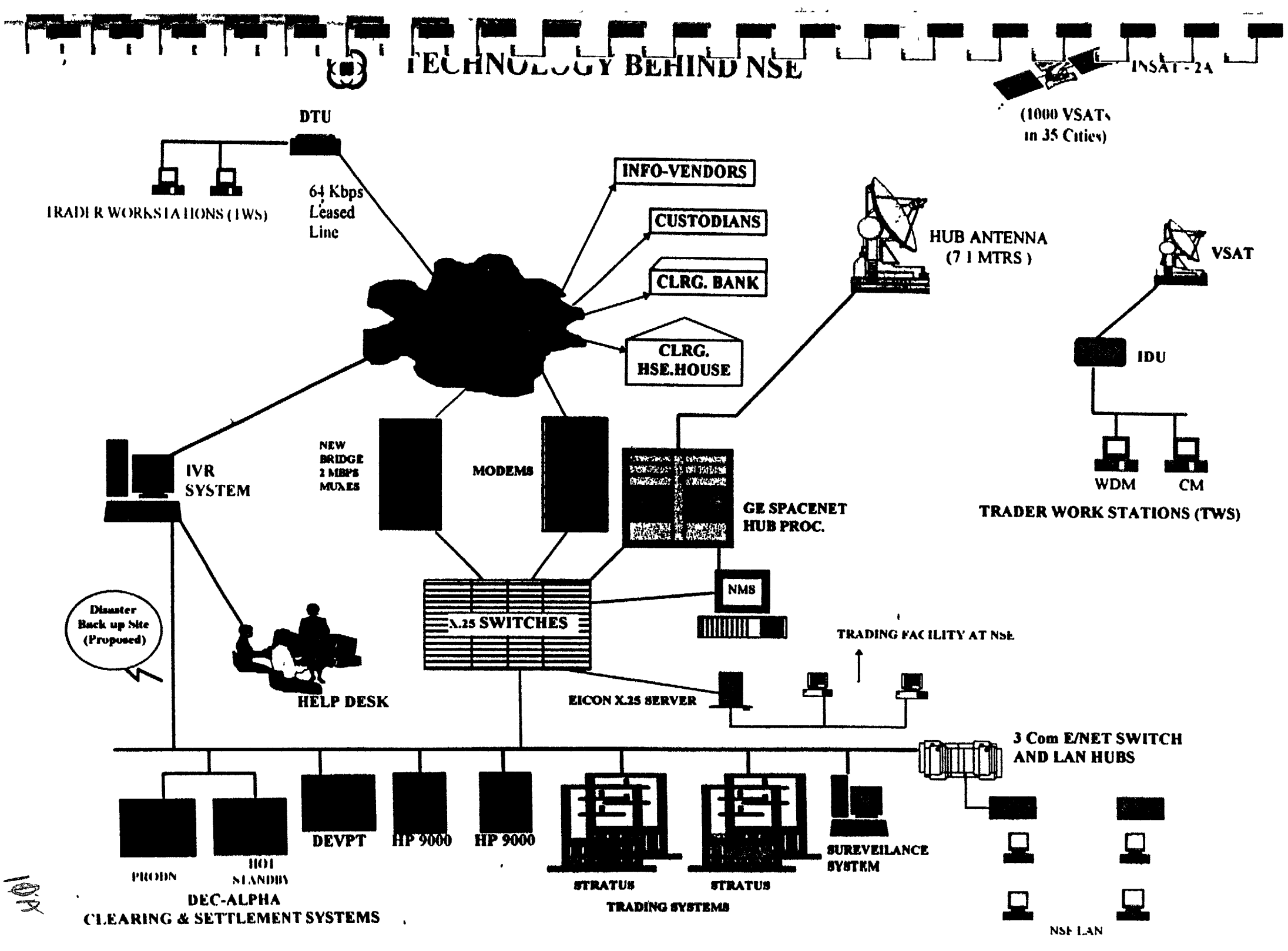

TABLE III- A-1- Threat Analysis

Department : Telecom

Threat : Failure of Satellite

Background and Current risk reduction measures :

The satellite connection is provided by the Department of Telecommunications (DOT) on the INSAT IIA. In case of failure of the satellite, alternative arrangement on another satellite needs to be provided by the DOT Such change shall involve change in the direction of Hub antenna as well as VSATs at the members end Hence the recovery of the satellite would take minimum of ten days

Even after the arrangement for a link through an alternate satellite, the entire network cannot be recovered upto 10 days from the day of such failure.

Further Countermeasures :

1 Currently, there is an arrangement with the DOT for an alternate satellite link However, the excat satellite has not been identified. The forthcoming satellite INSAT IID, which will be launched in middle of the year 1997, will be co-located with INSAT IIA. On allocation of the same space segment on INSAT IID, the recovery time from such a threat will be considerably reduced.

2. Markings on the antenna should be made for shifting it to face such alternate satellite Provide necessary training to the members to change the direction of the antenna

3. Motorised VSAT antenna may be installed at member locations as deemed fit by NSEIL to accommodate such change in satellite connection.

4 Members should be instructed about the necessary actions to be taken at their location/s in case of such a change.

TABLE III- A-1- Threat Analysis

Department : Telecom

Threat : Failure of Transponder

Background and Current risk reduction measures :

The satellite connection is provided by the Department of Telecommunications (DOT) on the INSAT IIA. In case of failure of the current transponder, alternative arrangement on another transponder on the same satellite need to be provided by the DOT This will involve a change of the satellite frequency and other parameters, which can be completed in a day's time

Currently there is no permanent backup transponder made available by the DOT

Even after the arrangement for another transponder on the same satellite, the entire network cannot be recovered within 24 hours from the time of such failure.

Further Countermeasures :

1 Arrangement should be made with the DOT for allotting a back up transponder

TABLE III- A-1- Threat Analysis

Department : Telecom

Threat : Failure of Antenna

Background and Current risk reduction measures :

The 7 6m Hub antenna installed at the Mahindra Towers premises of the NSEIL uplinks to the INSAT IIA satellite in the 6.764 GHz to 6 773 GHz and downlinks in the 4 539 GHz to 4 548 GHz The important components of the same are as below

1 Antenna Low Noise Amplifier (LNA)
2. Antenna Orthogonal Mode Transducer (OMT)
3 Antenna Wave guide

The minimum time for recovery from antenna failure is not less than three hours This three hours time includes the time required for testing and monitoring before uplinking.

Further Countermeasures :

1. Periodic checks should be initiated to eliminate the possibility of antenna failure.

2. Spares of critical components should be maintained Procedures should be laid down to ensure the availability and physical safety of such spares.

TABLE III- A-1- Threat Analysis

Department : Telecom

Threat : Failure of Radio Frequency Transreceiver (RFT) equipment

Background and Current risk reduction measures :

The RFT equipment installed at the Mahindra Towers premises are housed in a *"porta cabin"* and comprises of the following important components in hotstandby mode

1 RF Travelling Wave Tube Amplifier (TWTA) 400Wattts
2 RF Driver
3 RF Interface box for RF cables

The RF Protection Switching unit interconnects the two and provides auto/manual switching option.

The RF equipment is interconnected to the Hub baseband using the following ·

1. Inter Facility Link (IFL) Cable
2. RF Splitter (RCV path)
3. RF Combiner

Further Countermeasures :

1 Periodic checks should be initiated to eliminate the possibility of RFT failure.

2. Spares of critical components should be maintained at the NSEIL. Procedures should be laid down to ensure the availability and physical safety of such spares.

3 The IFL cable should be routed through different paths and through backup units

4 Backup units of the RF Splitter and RF Combiner should be maintained

TABLE III- A-1- Threat Analysis

Department : Telecom

Threat : Failure of Baseband equipment

Background and Current risk reduction measures :

The Hub baseband equipment provides access for the hosts/ servers attached to the X 25 network to get connected to the VSATs in the wide area network The baseband also converts this information to make it "satellite ready", which is then modulated for uplinking/ demodulated after reception and detection The same is then transported over the IFL cable to the RF equipment. The important components of the baseband are

1 Receiver cage Power Supply Unit (PSU)
2. Receiver cage (backplane)
3. Receiver card
4 Power Splitter
5 Hub Satellite Processing (HSP) cage (PSU)
6 HSP (Central Processing Unit)
7 HSP (Hard Disk Drive)
8. Modulator
9. Hub Protocol Processing (HPP) Cage (PSU)
10 Metacomp
11 Linear Area Network card
12. HPP Chassis (PSU)
13. Beacon Receiver
14. Autotracking unit
15. Patch Panel/ Cable

Further Countermeasures :

1. Spares of all critical components should be maintained Procedures should be laid down to ensure the availability and physical safety of such spares

2 A hotstandby with Matrix switching should be provided wherever applicable.

3 The supplier should be asked to provide hot swappable option for the Receiver card and there is a backup of HSP config data as well as redundant chain architecture to take care of the failure.

4 The supplier should be asked to provide Redundant architecture based on dual LAN cards per cage and dual PSU

TABLE III- A-1- Threat Analysis

Department : Telecom

Threat : Failure of Network Management System (NMS)

Background and Current risk reduction measures :

The actual control and monitoring of the VSAT network is possible using the NMS system which comprises of the following important components

1. Sun Sparc SS10 machine
2. NMS Software (proprietary to GE Capital Services Limited)
3. HDD
4. DAT

Currently the Sun machine is duplicated and adequate backup measures are taken to ensure that either of the machines can work The VSAT NMS currently works on a proprietary protocol to talk to it's components and does not support SNMP

Further Countermeasures :

1. Change the NMS to a fault tolerant machine with standardised protocol such as Simple Network Management Protocol (SNMP)

2 A backup of the software should be kept on site as well as off site

TABLE III- A-1- Threat Analysis

Department : Telecom

Threat : Failure of the MTNL, Worli Exchange

Background and Current risk reduction measures :

The MTNL, Worli Exchange is the Main Automatic (switching) eXchange (MAX) for all communication links from NSE to the outside switched world The links include voice and data circuits. This exchange is critical as the data links to the backup site as well as other offices of NSEIL for on-line host data backup and clearing activities are routed through the exchange

In case Mahindra Towers is not available the connectivity between Pune the backup site, and other offices of NSEIL involved in the clearing activities becomes vital. This vital communication link is through the Worli exchange

Currently, there are no provisions for alternate routing of links

Further Countermeasures :

Arrangement with the MTNL should be made for allotting alternate routing of links through another exchange, in case of failure of the Worli exchange

TABLE III- A-1- Threat Analysis

Department : Telecom

Threat : Failure of Air Conditioning units for the RFT cabin in Mahindra Towers

Background and Current risk reduction measures :

There are two Window AC units together with three Split AC units for the RFT cabin The air conditioning requirement is met by any three of the five AC units. The balance two AC units are redundant and can be utilised in case of failure of any of the AC units being used.

TABLE III- A-1- Threat Analysis

Department : Telecom

Threat : Failure of UPS for the Telecom equipment in the RFT cabin

Background and Current risk reduction measures :

The 15 KVA UPS unit consists of 2 units, one unit being the switching cubicle cum stabiliser, which is used to bypass raw power and the other, being charger cum inverter for the battery bank There is 1 set of battery bank. There is no automatic bypass to the entire unit failure.

In Mahindra Towers there are two UPS units taking over immediately in the event of a power failure. The UPSs have been configured to run in a parallel redundant mode In case of failure of one of the UPSs the full load is transferred to the running UPS Within 10 seconds of the UPS taking over, the diesel generators come on This covers the Telecom and other equipment, the computer room and the Stratus room. The UPSs are supplied by Tata Liebert and are currently under warranty support

Further Countermeasures :

1. Either a backup unit for the UPS or alternate source of UPS may be provided in the RFT cabin.

2 Automatic bypass arrangement should be made in case of failure of the entire UPS unit

TABLE III- A-1- Threat Analysis

Department : Telecom

Threat : Failure of Leased lines / DAMA VSATs in the Corporate Network

Background and Current risk reduction measures :

The 64 Kbps high speed intercity leased lines shall connect the Mahindra Towers office to the Regional offices Also, in certain cases, DAMA VSATs may be used for the same

Separately, it is proposed to have either a dial-up or a ISDN (subject to approval from DOT) connection for back-up purposes The permission for the same is sought from the DOT

TABLE III- A-1- Threat Analysis

Department : Telecom

Threat : Failure of Routers for the Corporate Network

Background and Current risk reduction measures :

It is proposed to install multiport to route data (essentially clearing, batch and LAN-to-LAN) over the leased lines / DAMA VSATs.

Further Countermeasures :

Spares of critical components should be maintained Procedures should be laid down to ensure the availability and physical safety of such spares.

TABLE III- A-1- Threat Analysis

Department : Telecom

Threat : Failure of Ethernet Switches / Hubs for the Corporate network

Background and Current risk reduction measures :

The Ethernet switches / hubs provide access to the LAN (on a case to case basis) LAN / Host data flows to and from these devices

Further Countermeasures :

Spares of critical components should be maintained Procedures should be laid down to ensure the availability and physical safety of such spares.

TABLE III- A-1- Threat Analysis

Department : Telecom

Threat : Failure of Multiplexers / EPAXs for the Corporate network

Background and Current risk reduction measures :

The multiplexers (if required) and the EPAXs provide voice communication essential for inter city operations.

Further Countermeasures :

Spares of critical components should be maintained Procedures should be laid down to ensure the availability and physical safety of such spares

For voice communication STD telephone lines can also be used.

TABLE III- A-1- Threat Analysis

Department : Telecom

Threat : Failure of NMS for the Corporate network

Background and Current risk reduction measures :

The NMS for the Corporate Network is essential for maintaining the country-wide leased lines / DAMA VSATs based network The NMS consists of the following

- Standard Server machine
- Network management software
- Network management tools

Further Countermeasures :

Spares of critical components should be maintained . Procedures should be laid down to ensure the availability and physical safety of such spares

TABLE III- A-1- Threat Analysis

Department : Telecom

Threat : Inadequate Capacity (bandwidth) of the satellite channels allotted by the DOT

Background and Current risk reduction measures :

Currently, there are four channels viz Outbound 1, Outbound 2, Outbound 3, Outbound 4 with the bandwidth of 128 Kbps each There is a Network Management System monitoring the traffic on each of these channels every fifteen minutes In case of excess load, the network would operate albeit with a reduced response time.

NSE is responsible for monitoring the capacity utilisation and immediate support from the systems and Capital Markets operations is provided in case of an emergency